

Patch Release Note

Patch SB251-13 For SwitchBlade 4000 Series Switches and AT-9800 Series Switches

Introduction

This patch release note lists the issues addressed and enhancements made in patch SB251-13 for Software Release 2.5.1 on existing models of SwitchBlade 4000 Series Switches and AT-9800 Series Switches. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch SB251-13.

Base Software Release File	sb-251.rez
Patch Release Date	08-Oct-03
Compressed Patch File Name	sb251-13.paz
Compressed Patch File Size	525044

This release note should be read in conjunction with the following documents:

- SwitchBlade Documentation Set for Software Release 2.5.1 (Document Number C613-03057-00 Rev A).
- AT-9800 Series Switches Documentation Set for Software Release 2.5.1 (Document Number C613-03056-00 Rev A)
- Release Note for Software Release 2.5.1 for SwitchBlade 4000 Switches and AT-9800 Series Switches (Document Number C613-10354-00 Rev D) available on the Documentation and Tools CD-ROM packaged with your switch, or from www.alliedtelesyn.co.nz/documentation/documentation.html.



WARNING: *Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.*

Some of the issues addressed in this Release Note include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

- Level 1** This issue will cause significant interruption to network services, and there is no work-around.
- Level 2** This issue will cause interruption to network service, however there is a work-around.
- Level 3** This issue will seldom appear, and will cause minor inconvenience.
- Level 4** This issue represents a cosmetic change and does not affect network operation.

Features in SB251-13

Patch SB251-13 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

- PCR: 02414** **Module: IPV6, SWI, IPG, VLAN** **Level: 2**
- MLD snooping is now supported on AT-9800 Series Switches. It is not available on the SwitchBlade. Refer to the section, *Multicast Listener Discovery (MLD) Snooping For SwitchBlade and AT-9800 Series Switches* shown at the end of the SB251-13 features.
- PCR: 03040** **Module: IPG** **Level: 3**
- Sometimes IP flows were not deleted correctly when both directions of the flow were in use. This issue has been resolved.
- PCR: 03524** **Module: OSPF, IPG** **Level: 2**
- OSPF was disabling RIP unless RIP was activated using the SET OSPF RIP command. This issue has been resolved.
- PCR: 03530** **Module: IPG** **Level: 2**
- Running the PURGE IP command with a multicast address and multiple sources was causing a fatal error. This issue has been resolved.
- PCR: 03542** **Module: HTTP** **Level: 3**
- The value specified for the IP parameter in the ADD FIREWALL POLICY PROXY command was not being used by the HTTP proxy. This issue has been resolved.
- PCR: 03598** **Module: ETH, IPG, IPv6, IPX, PORT, PPP.** **Level: 3**
- After about 250 days, commands such as SHOW BRIDGE COUNT were not displaying the correct number of seconds for *Uptime* and *Last Change At*. days. This issue has been resolved.

PCR: 03603 **Module: SWCX, SWI.** **Level: 3**

Ports on the SwitchBlade and AT-9800 are now initialised to advertise pausing as disabled.

PCR: 03606 **Module: IPG** **Level: 2**

BGP and UPNP were not informed when an ETH interface went up or down. This issue has been resolved.

PCR: 03609 **Module: OSPF, IPG** **Level: 1**

The IP route filter did not always work correctly for OSPF. This issue has been resolved.

PCR: 03617 **Module: FIREWALL** **Level: 2**

HTTP proxy did not discard cookies nor allow/deny access to URLs when a second pass on the URL was performed. This issue has been resolved.

PCR: 03643 **Module: CLNS/OSI** **Level: 3**

In a network with a large number of L1 intermediate systems (L1-ISs) a fatal error occurred after approximately 10 minutes. This issue has been resolved.

PCR: 03645 **Module: OSPF, IPG** **Level: 2**

Directed IPv6 PING messages were being transmitted from other interfaces if the specified interface was down. This issue has been resolved.

PCR: 03663 **Module: SWCX** **Level: 2**

When CAM segments were full, the CAM entries were not being moved correctly, and occasionally corrupting on compaction. This issue has been resolved.

PCR: 03668 **Module: SYSR** **Level: 2**

The SHOW SYS SYSR SLAVE command did not return a list of valid features. This issue has been resolved.

PCR: 03686 **Module: IPX** **Level: 3**

Entering the SHOW IPX CACHE command on the SwitchBlade or AT-9800 Series switches, was displaying a message stating that IPX route caching is not supported.

PCR: 03688 **Module: SYSR** **Level: 3**

This PCR, when introduced in Patch 12, resulted in the Master and Slave controller cards restarting whenever the bootscript contained more than 2000 VLANs. This issue has been resolved.

PCR: 03714 **Module: VLAN** **Level: 2**

The VLAN table was corrupting during a hot swap if a protocol or subnet VLAN had previously been created.

PCR: 03524 Module: OSPF, IPG Level: 2

The SET VLAN BCLIMIT command did not work when executed from start-up in a configuration script. This issue has been resolved.

PCR: 03717 Module: IP, SWCX Level: 2

New static routes cannot be added to the forwarding database until ARP has resolved the routes' next hop MAC address. In the meantime, selecting the best alternative route was sometimes causing incorrect forwarding and loops. To avoid this situation, packets destined for dead-end routes are now forced to the CPU. The CPU then creates an ICMP_Redirect message to the source of the unforwardable packet to remove the previous hop from its routing table.

In order to force packets back to the CPU, the hardware MAC table contains a special entry for each VLAN that maps the unused MAC address 55.55.55.55.55.55.55 to the Multicast Group ID 4096. When the switch encounters an unknown next hop MAC address, it now sends the packet to the L2MC Group 4096. Because this group does not exist, the packet is forwarded to the CPU. Note that this process will increment the SHOW SWITCH COUNTER command's L2MCGroupDoesntExist counter.

PCR: 03726 Module: TTY, USER Level: 3

When a user logged on twice, thus creating two sessions, the user log on time for the second session was overwriting the value recorded for the first. This issue has been resolved by displaying the log on times as two separate sessions.

PCR: 03727 Module: SWI, STP Level: 2

Previous STP ports were not being deleted correctly when line cards were hot swapped. Also STP ports were not initialising correctly when STP was not enabled. These issues have been resolved.

PCR: 03734 Module: IPG Level: 2

With static multicasting enabled on two VLANs, only the first few multicast packets of a stream were L3 forwarded. This issue has been resolved.

PCR: 03736 Module: IPG Level: 3

The copying of switch routes between internal components was causing processing delays. This issue has been resolved.

PCR: 03739 Module: SWI Level: 2

Although the SwitchBlade hardware is capable of forwarding jumbo frames, sending these to the CPU was causing a variety of issues. These issues have been resolved.

PCR: 03746 Module: BGP Level: 3

Attempts to disable BGP debug were, depending on configuration, resulting in either a system failure, or the debug messages continuing to appear after debug had been disabled. This issue has been resolved.

PCR: 03747 Module: VRRP Level: 3

An *unknown interface* log message was returned for VRRP if there was an interface UP or interface DOWN event due to a mismatch between a monitored interface index and the corresponding interface instance. This issue has been resolved.

PCR: 03751 Module: MLDS Level: 3

The MLD snooping entries registered on a port were not removed when the port went down or was unplugged. This issue has been resolved.

PCR: 03764 Module: IPG Level: 3

The IP multicast counter did not increment when IGMP, DVMRP and PIM packets were transmitted and received. This issue has been resolved.

PCR: 03769 Module: SWI Level: 2

An error occurred in the GUI if it had been in operation for more than 20 days. This issue has been resolved.

PCR: 03778 Module: FILE, INSTALL, SCR Level: 2

Files used during start up were backed up from NVS to FLASH even if they were already present in FLASH. This used up FLASH memory unnecessarily. This issue has been resolved so that files are only backed up when a copy does not already exist in FLASH.

PCR: 03780 Module: INSTALL Level: 3

If a configuration file had a long file name, the SHOW CONFIG command displayed the file name using the shortened DOS 8.3 format (where file names are 8 characters long, with extensions of 3 characters). This issue has been resolved so that long configuration file names are now displayed using the DOS 16.3 format (where file names are up to 16 characters long).

PCR: 03783 Module: IPG Level: 3

The TIMEOUT and SIZE parameters are only valid for the SET IP DNS CACHE command, but no error message was returned if either parameter was specified for the SET IP DNS command. This issue has been resolved.

PCR: 03784 Module: IPV6 Level: 3

Fragmentation of IPv6 packets now complies with RFC 2460's requirement to align packet sizes to 8 octets.

PCR: 03791 Module: SWCX Level: 2

Disabled copper ports on AT-SB4411 8-Port (RJ-45) Gigabit Ethernet Line Cards and AT-SB4441 8-GBIC Line Cards were not disabled on reboot. This issue has been resolved.

PCR: 03793 Module: RSVP Level: 3

The ENABLE RSVP INTERFACE command did not succeed if IP was enabled after the RSVP interface had been created. Now, ENABLE RSVP INTERFACE will succeed regardless of when IP is enabled as long as an IP interface exists.

PCR: 03795 Module: SWI Level: 3

Browsing the *dot1dTpFdbPort* table with SNMPv2c sometimes gave incorrect output. This issue has been resolved.

PCR: 03796 Module: STP Level: 2

Setting RSTPTYPE to NORMAL, when normal has already been set, sets all ports to the "sending RSTP" state process. This is referred to in IEEE 802.1w as *mCheck*.

When RSTPTYPE was changed from STPCOMPATIBLE to NORMAL with the SET STP command, the STP instance continued to send STP BPDUs until an *mCheck* was performed by entering the SET STP RSTPTYPE=NORMAL command again. This issue has been resolved so that when RSTPTYPE is set to NORMAL an *mCheck* is performed, causing the STP to start sending RSTP BPDUs immediately.

PCR: 03800 Module: LOAD Level: 2

If a DNS lookup failed when using the UPLOAD command to load a file with a host name, the file was sometimes deleted from FLASH. This issue has been resolved.

PCR: 03801 Module: MLDS Level: 2

MLD and MLD Snooping accepted MLD *Query* packets with a hop limit greater than 1. Duplicate packets were forwarded when the hop limit was not 1 and the payload was 0::0. This issue has been resolved. MLD and MLD Snooping now require the hop limit to be 1.

PCR: 03802 Module: FIREWALL Level: 1

Packets with bad ACK numbers were sometimes generated by the firewall as part of the proxy TCP setup process. These packets sometimes caused TCP sessions from the public side of the firewall to fail. This issue has been resolved.

PCR: 03806 Module: VRRP Level: 4

After the SHOW VRRP command was executed, incorrect trigger messages were entered into the log. This issue has been resolved.

PCR: 03811 Module: UTILITY Level: 2

A fatal error sometimes occurred when using hardware filters if DMA debug was enabled. This issue has been resolved.

PCR: 03813 Module: SWI Level: 2

Rate limiting sometimes prevented IGMP snooping and MLD snooping from operating correctly. This issue has been resolved.

PCR: 03814 Module: SWI Level: 1

A fatal error occasionally occurred because of an error with internal processing of the control blades. This issue has been resolved.

PCR: 03815 Module: SWI Level: 3

The SHOW SWITCH HOTSWAP command output displayed more than 4 blades on a 4 blade chassis. This issue has been resolved.

PCR: 03817 Module: IPV6 Level: 2

A fatal error occurred when IPv6 fragmented a packet. Also, when a large fragmented ICMP echo request packet was received, the reply may not have been fragmented and so may have exceeded the MTU for the interface it was sent on. These issues have been resolved.

PCR: 03819 Module: SWCX Level: 3

Previously, Multicast Storm Protection limited broadcast packets when Broadcast Storm Protection was not enabled. This has been changed so that *only* multicast packets are limited when Multicast Storm Protection is enabled, and *only* broadcast packets are limited when Broadcast Storm Protection is enabled.

PCR: 03821 Module: SWCX Level: 3

If a 10MB half-duplex link was connected to a port, the maximum bandwidth shown in the SHOW SWITCH TABLE command output was not updated. This issue has been resolved.

PCR: 03823 Module: VLAN Level: 2

If the last port in a VLAN went down, that port was not automatically deleted from IGMP groups. This issue has been resolved.

PCR: 03824 Module: IPG Level: 3

A multihomed interface sometimes sent duplicate multicast packets. This issue has been resolved.

PCR: 03825 Module: IPG Level: 2

The incorrect logical interface was selected for broadcast packets received with a subnet mask that differed from the class mask. This issue has been resolved.

PCR: 03826 Module: BGP Level: 2

When BGP imported routes from IP with the ADD BGP IMPORT command, and there were multiple import choices, the best IP route was not always imported. This issue has been resolved.

PCR: 03828 Module: IPV6 Level: 2

The MTU value for IPv6 PPP interfaces was always set to 1280 bytes. This MTU value is now correctly set to 1500 bytes, and 1492 bytes for PPP over Ethernet (PPPoE).

PCR: 03829 Module: SWCX Level: 3

The value of the *ifInErrors* counter in the SHOW INTERFACE=*interface* command incorrectly showed the number of packets received with bytes in the normal range. This issue has been resolved. The *ifInErrors* counter now correctly shows the number of packets received that had errors.

PCR: 03834 Module: SWCX Level: 2

Hardware filters using classifiers that specified IP addresses were not accepted by the ADD SWITCH HWFILTER command when added in a particular order. This issue has been resolved.

PCR: 03835 Module: VLAN Level: 3

If either the MCLIMIT or BCLIMIT parameter in the SET VLAN MCLIMIT BCLIMIT command was set to NONE, the other parameter was sometimes incorrectly set to NONE as well. This issue has been resolved.

PCR: 03836 Module: OSPF Level: 2

OSPF sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03837 Module: VLAN Level: 3

When browsing the *ifInNUcastPkt* MIB counter, the value was not correctly incremented because only broadcast packets were counted. This issue has been resolved.

PCR: 03839 Module: IPV6 Level: 2

A fatal error sometimes occurred when an IPv6 ping packet length exceeded 1453 bytes. This issue has been resolved.

PCR: 03841 Module: IPG Level: 2

A fatal error occurred when the PIM path was recovering. This issue has been resolved.

PCR: 03842 Module: IPG Level: 3

MLD startup query packets were not being sent correctly due to IPv6 MLD being unaware of the IPv6 interfaces it was running on. This issue has been resolved.

PCR: 03843 Module: DHCP Level: 2

When some DHCP entries were in *Reclaim* mode, and all interface links related to the range of these entries went down, these DHCP entries were stuck in *Reclaim* mode. This issue has been resolved.

PCR: 03846 Module: SWCX Level: 2

An STP blocking port did not discard SNAP encapsulated packets with TYPE=00BB (ESRP packets). This caused a loop in the network. This issue has been resolved.

PCR: 03849 Module: SYSR Level: 2

The GUI install file was not copied to the slave controller card after executing the SET INSTALL=GUI command. This issue has been resolved.

PCR: 03850 Module: FFS Level: 3

Files were not displayed in the SHOW FFILE command output, after entering “Q” at the CLI to quit from a previous prompt. This issue has been resolved.

PCR: 03853 Module: SWCX Level: 2

Multicast packets were not forwarded between switch instances on SwitchBlade series switches. This issue has been resolved.

PCR: 03855 Module: IPG Level: 2

Previously, an IP multicast stream destined for an IP multicast group was forwarded out ports in the All Groups IGMP snooping entry even after this entry had timed out. This issue has been resolved.

PCR: 03857 Module: SWCX Level: 1

When a GBIC port had its speed and duplex configured as part of a configuration script, the settings were not applied to the hardware. This issue has been resolved.

PCR: 03859 Module: SWI Level: 2

The speed on copper GBIC ports can no longer be manually set.

PCR: 03861 Module: SWI Level: 2

When linking up a single interface.

PCR: 03861 Module: IPV6 Level: 2

When a connector was plugged into one physical interface, the RIPng request packet was erroneously transmitted from all interfaces on the switch. This issue has been resolved.

PCR: 03864 Module: BGP Level: 2

BGP sent *Update* packets when the local host route table changed but did not affect BGP. Also, BGP did not send *Withdrawn* packets when there was a change in the best route. These issues have been resolved.

PCR: 03865 Module: FIREWALL Level: 2

When dual firewall policies were defined, public to private passive mode FTP transfers sometimes failed. This issue has been resolved.

PCR: 03867 Module: BGP Level: 2

BGP sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03869 Module: CFLASH Level: 3

CompactFlash™ cards formatted to FAT16 by Windows XP were not recognised correctly. This was because Windows XP reserved a number of sectors. This issue has been resolved.

PCR: 03872 **Module: SWI** **Level: 3**

When typing “?” at the command line after SET SWITCH PORT, INGRESSLIMIT was incorrectly displayed as a valid option. This issue has been resolved.

PCR: 03879 **Module: DHCP** **Level: 2**

A memory leak was occurring with DHCP. This issue has been resolved.

PCR: 03880 **Module: SWICX, SWI** **Level: 2**

Unplugging the remote receive port on the 32FX card (AT-SB4352) was causing the switch to lock-up. This issue has been resolved.

PCR: 03887 **Module: SWCX** **Level: 2**

When the speed and duplex settings of a port were configured with the SET SWITCH PORT SPEED command, the port sometimes erroneously advertised auto-negotiation capabilities, usually when ports were configured with a startup script. This issue has been resolved so that switch ports will not advertise any capabilities when configured with fixed speed and duplex settings.

PCR: 03888 **Module: DHCP, TELNET** **Level: 2**

When the device was configured as a DHCP server, a fatal error sometimes occurred when a Telnet session to the device was closed while DHCP was reclaiming IP addresses. Also, a Telnet error message displayed an incorrect value when a telnet command line parameter was repeated (for example, SHOW TELNET TELNET). These issues have been resolved.

PCR: 03889 **Module: IPV6** **Level: 2**

Packets were not routed when an IPv6 flow was enabled. This issue has been resolved.

PCR: 03890 **Module: IGMP, SWI** **Level: 2**

The switch was adding a router port for multicast packets to destinations with an address in the range 224.0.0.x. Switch port entries are now only created for special router multicast addresses.

PCR: 03891 **Module: CORE** **Level: 3**

When the configurable temperature threshold had not been set, its value should show as “Undefined” in the output of the SHOW SYSTEM command, but it showed the same value as the fixed temperature threshold. This issue has been resolved.

PCR: 03899 **Module: CORE** **Level: 2**

A fatal error sometimes occurred during persistent hotswapping of line cards if the cards were inserted or removed before waiting for a message like the following examples to appear:

```
Info (1034266): Board AT-SB4411 8-1000T(RJ45) hot-inserted
```

```
Info (1034268): Board AT-SB4411 8-1000T(RJ45) hot-swapped out
```

This issue has been resolved.

PCR: 03907 **Module: IPV6** **Level: 2**

The CREATE CONFIG command did not generate the TYPE parameter for ADD IPV6 INTERFACE commands. This issue has been resolved.

PCR: 03913 **Module: SWCX** **Level: 2**

A fatal error occurred with NVS when the log contained too many debug log messages. These messages were added with PCR 03701. This issue has been resolved.

PCR: 03921 **Module: IP, ARP** **Level: 2**

The switch was previously responding to ARP request packets received with invalid (i.e. broadcast or multicast) source MAC or IP addresses. This issue has been resolved so that ARP packets received with broadcast or multicast MAC or IP addresses will be discarded.

PCR: 03922 **Module: PIM** **Level: 3**

The SET PIM INTERFACE command did not succeed when the HELLOTIMER parameter was specified. This issue has been resolved.

PCR: 03923 **Module: CORE** **Level: 3**

The AT-SB2415 Bandwidth Expander line card displayed an incorrect ID name in the output of the SHOW SYSTEM command. This issue has been resolved.

PCR: 03925 **Module: IPV6** **Level: 3**

Incorrect debug information was returned when an ICMPv6 *PacketTooBig* message was received. This issue has been resolved.

PCR: 03931 **Module: IPSEC** **Level: 3**

The IPsec configuration was not created correctly when the RADDRESS and LNAME parameters in the CREATE IPSEC POLICY command were used together. This issue has been resolved.

PCR: 03934 **Module: IPSEC** **Level: 2**

The CREATE IPSEC POLICY command failed if the interface specified with the INTERFACE parameter did not have a global IPv6 interface defined. This PCR implements a workaround by using the interface's link-local IPv6 address if no other IPv6 address can be found.

PCR: 03935 **Module: IPV6** **Level: 3**

ISAKMP debug messages now correctly outputs IPv6 addresses when using IPv6, and IPv4 addresses when using IPV4.

PCR: 03939 **Module: IPV6** **Level: 2**

When a *NeighbourAdvert* message containing an anycast target address was received, the device incorrectly performed Duplicate Address Detection. This issue has been resolved.

PCR: 03954 **Module: IPV6** **Level: 2**

Prefixes of Anycast addresses could not be shared on the same port. This issue has been resolved.

PCR: 3956 Module: SWI, CORE Level: 2

On an AT-9800 with certain third party GBICs, running the restart reboot command would cause the switch to lock-up. However the problem did not occur when using the Reset button. This issue has been resolved by disabling all ports before performing a RESTART REBOOT.

PCR: 03965 Module: IPSEC Level: 2

IPv6 was using the same SA (security association) soft expiry timer at both ends of link. This was wasting CPU and memory resources. This issue has been resolved.

PCR: 03966 Module: MLDS Level: 2

A multicast listener discovery (MLD) snooping entry was incorrectly added to the SwitchBlade's layer two multicast address table.

The AT-9800 was not adding layer two MLD Snooping when additional VLANs were created.

The failure of a SwitchBlade port was causing restarts due to the switch attempting to remove the port from a "non existent" MLD Snooping list.

These three issues have been resolved.

PCR: 03968 Module: OSPF Level: 2

Large routing areas, containing many hosts and interfaces, were causing fatal errors due to the excessive number of link state advertisements generated. This issue has been resolved by limiting the combined number of routers and hosts within each area to 100.

PCR: 03973 Module: SWI Level: 3

The IP option field for trace route was not being filled correctly when equal cost multipath routes were used. This has now been fixed.

PCR: 03986 Module: BGP, IPG Level: 2

Route flapping was occurring when an interface went down and there was another path to the *next hop*. This issue has been resolved.

PCR: 03991 Module: CFLASH Level: 2

A fatal error would occur if a file whose name contained Japanese characters was deleted from compact flash. This issue has been resolved.

PCR: 03991 Module: SWCX, SWI Level: 2

In configurations containing many VLANs, temporary lockups were frequently occurring while the hardware tables were being updated. This patch substantially reduces the severity of these lockups.

PCR: 031000 Module: SWCX, SWI Level: 3

Running the SHOW IP IGMP COUNTER command was displaying zero values for the *outQuery* and *outTotal* counters. This issue has been resolved.

PCR: 031003 Module: QOS Level: 3

The SET QOS VLANREMAP command was incorrectly saving configuration files. This was resulting in errors occurring when the file was executed. This issue has been resolved so that the file is saved in the correct form.

PCR: 031005 Module: SWCX Level: 3

CAM errors were appearing when the ENABLE SWITCH BIST command was run multiple times. This issue has been resolved.

PCR: 031006 Module: STP SWI Level: 2

When line cards were hotswapped, the card's STPs were not being correctly reset to indicate that the card had been exchanged. This sometimes resulted in a failure to select the preferred link, during the link re-establishment phase. This issue has been resolved.

PCR: 031007 Module: CFLASH Level: 2

On the AT-9800, files with no extension were causing fatal errors when stored on compact flash cards. This issue has been resolved to ensure that these files are handled correctly.

PCR: 031008 Module: CFLASH INSTALL Level: 2

On the AT-9800, the configuration file could be set from compact flash files held in directories other than the root. This issue has been resolved by preventing the configuration being set from files other than those located in the root directory.

PCR: 031012 Module: PIM Level: 2

The *prune* time limit was not being cancelled when an IGMP join was received by the switch. This was forcing the switch to send a Graft message in the upstream direction. This issue has been resolved by cancelling the prune time limit whenever an IGMP join is received.

PCR: 031014 Module: SWCX Level: 2

When the SWITCH PORT command parameters, 10HMAUTO, 10MFAUTO, 100MFAUTO etc, were used to set a port to auto negotiate at a particular speed, the port speed would not be retained following a card hot swap. This issue has been resolved.

PCR: 031015 Module: STP Level: 2

The PORT and PORTPRIORITY parameters of the STP PORT command were not always updating switch instances on ports that are members of multiple STP instances. This issue has been resolved.

PCR: 031020 Module: PIM Level: 2

When the switch received a generation ID change message, it was not responding by sending a PIM HELLO message. This issue has been resolved.

PCR: 031030 Module: SWCX Level: 3

BIST failures were occurring because the software was not full supporting the SwitchBlade 8 port 1000BASE-LX line card 1 (AT-SB4462). This issue has been resolved.

PCR: 031033 Module:

Level: 2

STP was not being handled correctly when hot swapping line cards. This resulted in links other than the preferred link being selected.

Also, when a layer two data stream was forwarded from one line card (the source card) to another (the destination card) via the preferred STP link, if the destination card had been swapped out, and the backup link was via the source card, then the data stream would not be forwarded correctly over the backup link.

These issues have been resolved.

Multicast Listener Discovery Snooping

Multicast Listener Discovery (MLD) snooping enables the switch to forward IPv6 multicast traffic intelligently, instead of flooding it out all ports in the VLAN.

Without MLD snooping, multicast group membership for VLAN aware devices is on a per-VLAN basis, because MLD is an IPv6-based protocol. If at least one port in the VLAN is a member of a multicast group, and MLD snooping is not used, IPv6 multicast packets will be flooded onto all ports in the VLAN. With MLD snooping, the switch passively listens to MLD joins / reports and leaves / done messages, to identify the switch ports that have received joins and/or leaves from devices attached to them. Multicast traffic will only be forwarded to those ports. MLD snooping will also identify ports that are connected to another router or switch and forward messages out those ports appropriately.

MLD snooping is performed at Layer 2 on VLAN interfaces automatically. By default, the switch will only forward traffic out those ports with routers or IPv6 multicast listeners, therefore it will not act as a simple hub and flood all IPv6 multicast traffic out all ports. MLD snooping is independent of the MLD and Layer 3 configuration, so an IPv6 interface does not have to be attached to the VLAN, and MLD does not have to be enabled or configured. MLD is described in the “*IPv6 Multicasting*” chapter of the AT-9800 Series Switch Software Reference.

MLD snooping will not generate MLD query messages, but will relay MLD queries from other routers or switches attached to one of its ports to other ports in the same VLAN.

MLDv2 supports Multicast Address and Source Specific messages. These messages enable a host to listen to traffic from a particular source to a particular multicast address, instead of all traffic for the group. MLD snooping cannot snoop these messages, because the address information is contained within the packet's IPv6 Layer 3 header. These messages will be flooded to all ports in the VLAN. The switch will snoop MLDv1 message types 130 (Query), 131 (Listener Report) and 132 (Listener Done), as specified in RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*, October 1999.

Multicast group membership registration entries on the switch will time out after no data or messages have been received for that group on that port for 270 seconds.

The following multicast addresses are used by IPv6 for special purposes, and will always be flooded:

```
FF02::1 (All nodes)
FF02::2 (All routers)
FF02::4 (DVMRP)
FF02::5 (OSPF/IGMP)
FF02::6 (OSPF/IGMP Designated routers)
FF02::9 (RIPv2)
FF02::d (PIM)
FF02::f (CBT)
FF02::12 (VRRP)
```

MLD snooping on the switch uses the last 4 bytes of the IPv6 address to distinguish multicast addresses. It is therefore unable to distinguish different multicast addresses that end with the same 4 bytes. Creating an entry for a multicast group will have the effect of creating an entry for all groups with addresses that end with the same 4 bytes as that group's address. For example, traffic for the groups:

```
ffxx xxxx xxxx xxxx xxxx xxxx 1234 5678 and
```

```
ffyy yyyy yyyy yyyy yyyy yyyy 1234 5678
```

will be forwarded out the same set of ports, irrespective of the values of x and y. Therefore, if MLD snooping is used, no two groups within the multicast domain should be given an address that ends in the same 4 bytes.

Similarly, all addresses beginning with ff02 and ending with any of:

```
0000:0001, 0000:0002, 0000:0004, 0000:0005, 0000:0006,  
0000:0009, 0000:000d, 0000:000f or 0000:0012
```

will be flooded out all ports in the VLAN, because MLD snooping cannot distinguish them from IPv6 special addresses. These addresses should be avoided if MLD snooping is used.

MLD snooping is enabled by default. To disable it, use the command:

```
DISABLE MLDSNOOPING
```

Note that IPv6 multicast packets will flood the VLAN when MLD snooping is disabled. Disabling MLD snooping may be useful on Rapier i Series Switches if filters are used extensively, because MLD snooping uses a Layer 3 filter. When MLD snooping is disabled, this filter becomes available. See *"Hardware Packet Filters"* in the *Switching* chapter of the Software Reference for information about filters.

To enable MLD snooping, use the command:

```
ENABLE MLDSNOOPING
```

MLD snooping can only be enabled if a free filter entry is available.

To display debugging information, use the command:

```
ENABLE MLDSNOOPING DEBUG
```

This command displays the ports that are currently receiving MLD packets and the ports that are being added or taken off the switch's multicast group membership registration.

To disable debugging, use the command:

```
DISABLE MLDSNOOPING DEBUG
```

To display information about MLD snooping, use the command:

```
SHOW MLDSNOOPING [COUNTER]
```

Example output from the SHOW MLDSNOOPING command is described in Figure 1 on page 17 and Table 1 on page 18. Example output from the SHOW MLDSNOOPING COUNTER command is described in Figure 2 on page 18 and Table 2 on page 18.

Figure 1: Example output from the SHOW MLDSNOOPING command.

```
MLD Snooping
-----
Status ..... ENABLED
Debugging ..... DISABLED
Group Timeout ..... 270 Secs

Interface: vlan1
-----
Multicast Address ..... ff05:2222:3333:4444:5555:6666:7777:1111
Ports ..... 1,2,4-6
Entry Timeout ..... 120 Secs

Multicast Address ..... All routers group
Ports ..... 5
Entry Timeout ..... 208 Secs

Interface: vlan4
-----
Multicast Address ..... ff01:1234:1234:5678:5678:2222:1111:3333
Ports ..... 12,13,14
Entry Timeout ..... 56 Secs
```

Table 1: Parameters displayed in the output of the SHOW MLDSNOOPING command.

Parameter	Meaning
Status	The status of MLD snooping; one of ENABLED or DISABLED.
Debugging	The status of MLD snooping debugging; one of ENABLED or DISABLED.
Group Timeout	The switch's timeout period for multicast group registration (270 seconds). If no MLD listener joins are received during this period of time, the group registration will be deleted.
Interface	The interface for which multicast registrations are displayed.
Multicast Address	The IPv6 multicast group address registered for a particular VLAN interface.
Ports	The member ports for the multicast group.
Entry Timeout	The number of seconds remaining until this multicast registration will be deleted if no listener joins are received.

Figure 2: Example output from the SHOW MLDSNOOPING COUNTER command.

```

MLD Snooping Counters
-----
InMessages ..... 52
InDiscards ..... 2
InGenQueries ..... 10
InSpecQueries ..... 4
InJoins ..... 20
InDones ..... 16
-----

```

Table 2: Parameters displayed in the output of the SHOW MLDSNOOPING COUNTER command.

Parameter	Meaning
InMessages	The number of MLD messages received by the CPU on the switch.
InDiscards	The number of MLD messages received by the CPU on the switch but discarded, for example, because the packets were malformed.
InGenQueries	The number of MLD general query messages received the CPU on the switch.
InSpecQueries	The number of MLD specific query messages received the CPU on the switch.
InJoins	The number of MLD listener joins messages received the CPU on the switch.
InDones	The number of MLD listener done messages received by the CPU on the switch.

Features in SB251-12

Patch SB251-12 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:



After loading this software version, please check your alarm relay connections. Refer to PCR 03209 for more information.

PCR: 03287 Module: Firewall Level: 2

When configured with ACTION=NAT, the firewall was incorrectly applying TCP port filtering. This issue has been resolved. Also, the GBLPORT parameter of the commands, SET FIREWALL POLICY RULE and ADD FIREWALL POLICY RULE is no longer applied when ACTION is set to NAT.

PCR: 03437 Module: IPV6 Level: 2

RIP was learning routes from neighbours even when it was disabled. This issue has been resolved.

PCR: 03661 Module: SWCX Level: 2

Traffic that matched the internal system rules in the Packet Classifier tables was not always being directed to the same internal traffic class. This issue has been resolved.

PCR: 03688 Module: SYSR Level: 2

In configurations using two switch controller cards, the system redundancy feature (SYSR) could not locate and initialise the second switch control card. This issue has been resolved.

PCR: 03715 Module: SWI Level: 2

ESRP™ packets received were being dropped and not forwarded. This issue has been resolved.

PCR: 03733 Module: IPV6 Level: 3

When an oversize packet (PMTU) was received, an error message was not returned, even when IPv6 flow was enabled. This issue has been resolved.

PCR: 03744 Module: IPG, SWCX Level: 3

Entering the command PING 0.0.0.0 was not producing an error message. Also, the TRACE function was not resolving local addresses correctly. These issues have been resolved.

PCR: 03750 Module: IPv6 Level: 3

The IPv6 loopback address was used as a source address in ping packets, causing ping to fail. This issue has been resolved.

PCR: 03756 Module: IPV6 Level: 2

The following issues have been resolved:

- IPv4 addresses x.x.x.0 or x.x.x.255 were not accepted for the IP parameter in the ADD IPV6 6TO4 command.

- IPv4 addresses x.x.x.0 or x.x.x.255 were not accepted for the LOCAL parameter in the ADD IPV6 TUNNEL command.
- IPv6 addresses 2002:x:x::/48 were not accepted for the IPADDRESS parameter in the ADD IPV6 INTERFACE command.

PCR: 03760 **Module: SWI** **Level: 1**

Changes have been implemented to prevent loss of connectivity between line cards.

PCR: 03763 **Module: SWI** **Level: 2**

When port speeds were set using a configuration script, their capabilities on line cards with CAM, were being incorrectly reported. This issue has been resolved.

PCR: 03770 **Module: SWI** **Level: 2**

The SwitchBlade SB4108 chassis was failing the L3 Full Mesh test. This issue has been resolved.

PCR: 03773 **Module: SWI** **Level: 3**

The SHOW SYSTEM command was not correctly displaying the Compact Flash patch files.

PCR: 03775 **Module: SWI** **Level: 2**

Fatal errors were occasionally occurring when multicast forwarding was updated. This issue has been resolved.

PCR: 03777 **Module: QOS** **Level: 2**

If a SET operation failed, the recovery process applied the default MAXBANDWIDTH setting, regardless of either the configured value, or the port speed capability. This was resulting in the MAXBANDWIDTH value being too high. This issue has been resolved.

PCR: 03782 **Module: QOS** **Level: 3**

Additional messages will now advise the file transfer status as files are transferred between compact flash and flash memory.

PCR: 03794 **Module: SWI** **Level: 2**

The SwitchBlade, SB4104 chassis, was failing the L3 Full Mesh test. This issue has been resolved.

PCR: 03797 **Module: SWI** **Level: 1**

IPX routing did not work in certain circumstances. This issue has been resolved.

PCR: 03188 **Module: IPG, SWI, VRRP** **Level: 3**

For switches configured for VRRP, it was not possible to Ping the switch operating in the Master state. This issue has been resolved.

PCR: 03189 **Module: FIREWALL, LB** **Level: 3**

A fatal error occurred in the load balancer when there were no UP resources in a resource pool. This issue has been resolved. Load balanced TCP

connections will now only retry SYNs once after 5 seconds. The round robin selection algorithm will now select an UP resource in a resource pool with only one UP resource, even if it was used for the last successful connection.

PCR: 03194 Module: LB Level: 3

Sometimes healthcheck pings were not sent to the load balancer resources. This issue has been resolved.

PCR: 03196 Module: IPV6 Level: 3

The system became unstable if the ADD IPV6 TUNNEL command failed. This instability was caused by the partially created tunnel entry not being properly removed from the tunnel database. The tunnel entry is now completely removed.

PCR: 03199 Module: IPV6 Level:

Invalid routes and packets were occurring within RIP. This issue has been resolved.

PCR: 03201 Module: SWI Level: 4

AT-9800 Series switches with 16 ports could be configured beyond their 16 port maximum. Attempting to configure port 17 would produce no error message, and attempting to configure ports 18 and above would result in an incorrect error message. Also, the SwitchBlade could be allocated with 17 ports within a single trunk group, one port more than the maximum. These issues have been resolved; in both instances the maximum port configuration is now 16.

PCR: 03203 Module: IPV6 Level: 3

RIPng was not sending a response back to a RIP request message. This issue has been resolved.

PCR: 03206 Module: IPG Level: 3

IPv4 filters now behave like IPv6 filters.

PCR: 03207 Module: Alarm Level: 4

The SHOW SYSTEM SYSR SLAVE COUNT and SHO SYS SYSR SLAVE commands have been removed from the user command set.

PCR: 03208 Module: FIREWALL Level: 2

When the configuration script was created using the CREATE CONFIG command, the GBLIP parameter in the ADD FIREWALL POLICY command was listed twice. This caused the command to fail when the device was restarted. This issue has been resolved.

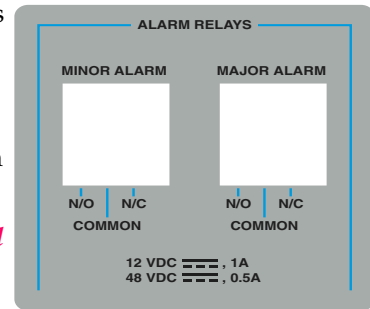
PCR: 03209 MODULE: ALARM**Level: 1**

The action of the MAJOR and MINOR relays does not presently match the illustration located alongside their connections.

This issue has been resolved by reversing the action of the relays in software to match the illustration shown on the right.



Please check that your alarm relays are still appropriately connected.

**PCR: 03210 Module: PING****Level: 4**

The SET TRACE PORT command was not functioning correctly. Also, the SHOW CONFIG DYNAMIC PING command was producing an incorrect output format. These issues have been resolved.

PCR: 03212 Module: IPV6**Level: 3**

The TRACE command was not working when using an IPv6 link-local address. This issue has been resolved.

PCR: 03213 Module: IPSEC**Level: 3**

A memory leak occurred when some IPSEC processes failed. This issue has been resolved.

PCR: 03214 Module: PIM**Level: 2**

Parallel forwarding PIM neighbours were not always sending PIM *Assert* messages following a neighbour re-boot. This was causing the transmission of duplicate multicast data. This issue has been resolved.

PCR: 03216 Module: PIM, PIM6**Level: 2**

PIM4 and PIM6 were not sending *Hello* packets if the HELLOINTERVAL was not a multiple of 10. This is set with the ADD PIM INTERFACE, ADD PIM6 INTERFACE, SET PIM INTERFACE, and SET PIM6 INTERFACE commands. This issue has been resolved.

PCR: 03217 Module: DVMRP**Level: 2**

If a DVMRP interface was deleted and then added again, DVMRP routes associated with this interface were not reactivated. This issue has been resolved.

PCR: 03222 Module: PIM, PIM6**Level: 2**

If the RP candidate advertising time was set to a non-default value with the ADVINTERVAL parameter in the SET PIM command, the hold time in the message was not being updated correctly. This issue has been resolved.

PCR: 03223 Module: SWI**Level: 2**

The output from the SHOW SWITCH PORT COUNTER command was showing incorrect values for packets greater than 1519 bytes. This issue has been resolved.

PCR: 03224 Module: IPG Level: 2

If an IP address was added using the AD IP INTERFACE IP=DHCP and the server could not assign an IP address due to a network problem affecting the server's VLAN, any further frames transmitted to IP addresses on other VLANS would be blocked. This issue has been resolved.

PCR: 03227 Module: SWI Level: 4

Previously, the default output of the SHOW SWITCH FDB command displayed the forwarding database information for ports on the controller card located in bay A. The default now displays all external ports for switch instances except for those on the controller card. This command no longer displays information about internal ports.

PCR: 03229 Module: LOAD Level: 3

Zmodem was not naming some loaded files. This issue has been resolved.

PCR: 032231 STP Level: 3

STP was advertising an incorrect length for BPDU packets. This issue has been resolved.

PCR: 03232 Module: BGP Level: 3

Values for the KEEPALIVE and HOLDDTIME parameters in the ADD BGP PEER and SET BGP PEER commands were not interacting correctly. This issue has been resolved.

PCR: 03234 Module: IPG Level: 3

The PURGE IP command did not remove ENABLE IP IGMP from the configuration. This issue has been resolved.

PCR: 03236 Module: IPG Level: 3

IGMP queries were being sent after IGMP was disabled. This issue has been resolved.

PCR: 03237 Module: IPG Level: 2

RIP *Request* packets for IPv4 were not being transmitted when the link came up or when the switch restarted. This issue has been resolved.

PCR: 03238 Module: SWI Level: 2

When RIP interfaces were deleted, the IP routes learned through those interfaces were not timing out correctly. Now, all IP routes learned through a RIP interface are removed when the RIP interface is deleted, and no timeouts occur.

PCR: 03239 Module: QOS Level: 2

QoS Traffic Class maximum bandwidth limiting was being overwritten by the port or trunk maximum bandwidth value. This should only happen when the Traffic Class maximum bandwidth has *not* been set manually with

the CREATE QOS TRAFFICCLASS MAXBANDWIDTH parameter. This issue has been resolved.

PCR: 03240 Module: OSPF Level: 2

A fatal error occurred when OSPF was under high load. This issue has been resolved.

PCR: 03244 Module: ETH, IPG Level: 3

ARP table entries are now deleted when an ETH interface goes down.

PCR: 03245 Module: SWI, IPG, PIM Level: 2

Multicast streams would not commence forwarding immediately due to IGMP packets initiated but not sent while a VLAN was changing from the DOWN to UP state. Also, multicast streams could be received while the VLAN was changing from DOWN to UP, causing a PIM Reverse Path Forwarding unicast route lookup failure. This was due to the unicast route being unusable as the VLAN was still considered down. These issues have been resolved.

PCR: 03246 Module: SWI Level: 3

For the SwitchBlade and AT-9800 Series Switches, the TTL egress limit for forwarding IP multicast packets has been increased from 0 to 1. Therefore, only packets with a TTL greater than 1 will be forwarded.

PCR: 03248 Module: VLAN Level: 4

The error message for an incorrectly added or removed port now displays both the card and the port identifiers.

PCR: 03250 Module: SWI Level: 4

The DELETE SWITCH FILTER command did not work properly when the ENTRY parameter was assigned a range with hyphen ("-"). This issue has been resolved.

PCR: 03252 Module: PIM Level: 3

An assert storm sometimes occurred with PIM-DM. This issue has been resolved.

PCR: 03254 Module: BGP Level: 2

If, with one or more routes already configured, BGP was enabled and an additional route added, BGP was not aggregating the new route. This issue has been resolved.

PCR: 03256 Module: MLD Level: 3

MLD did not respond correctly when it was in *exclude* mode and it received a request block. This issue has been resolved.

PCR: 03257 Module: SWI Level: 2

When using the SET SWITCH PORT command, setting port intrusion caused static MAC addresses to be deleted. This issue has now been resolved.

PCR: 03260 **Module: SWI, SNMP** **Level: 4**

The SNMP MIB browser was returning nonaligned pairs following a *GetNext* of the FDB table. This issue has been resolved.

PCR: 03261 **Module: VLAN, IPG** **Level: 4**

VLAN and IPG packet debugging facility has now been restored.

PCR: 03262 **Module: PPP** **Level: 3**

The CREATE CONFIGURATION command adds the PPP TEMPLATE LQR parameter when LQR is enabled. But the configuration script always contained "LQR=ON" even when the LQR value was not the default. This issue has been resolved.

PCR: 03263 **Module: SWI** **Level: 4**

The EGRESS parameter setting was not displayed by the SHOW CONFIG DYNAMIC command. This issue has been resolved.

PCR: 03265 **Module: SWI** **Level: 3**

The IFHC counter used within the SNMP MIB was producing incorrect counts. This issue has been resolved.

PCR: 03266 **Module: PIM** **Level: 2**

The handling of the upstream neighbour for a *GraftACK* message has been corrected.

PCR: 03273 **Module: ALARM** **Level: 4**

The PORT parameter of the ADD ALARM command would not accept a range of ports. This issue has been resolved.

PCR: 03274 **Module: SWI** **Level: 4**

Entering the command, SET SWITCH TRUNK SPEED was returning the inappropriate error message, "The INSTANCE specified does not exist." This issue has been resolved.

PCR: 03275 **Module: SWI** **Level: 2**

On SwitchBlade and AT-9800 Series switches, adding a static ARP entry resulted in the entry of the MAC address being added for the next hop port. These addresses were being incorrectly added if the next hop port was configured as a tagged port. This issue has been resolved.

PCR: 03278 **Module: IPV6** **Level: 4**

The timing of LLQ packets has been modified to be consistent with MLD Draft (Nov 2002).

PCR: 03280 **Module: IPG, BGP** **Level: 1**

BGP/IPG was causing fatal errors to occur following network topology changes. This issue has been resolved.

PCR: 03285 **Module: IPG** **Level: 4**

RIP packets can now contain up to 25 routes per packet instead of 24.

PCR: 03288 Module: L2TP Level: 2

When a radius lookup performed by the L2TP Access Concentrator (LAC) failed, the LAC attempted to disconnect the call from its tunnel. If the tunnel had not been created, the device restarted. This issue has been resolved.

PCR: 03290 Module: SWI Level: 2

PINGING between blades within the same switch failed whenever the current master was located in the right-hand slot and a control blade was located in the left-hand slot. This issue has been resolved.

PCR: 03291 Module: PPP Level: 2

A PAP authentication failure with PPPoE could cause a fatal error. This issue has been resolved.

PCR: 03293 Module: PPP Level: 3

The MAXSESSION parameter of the SET PPP ACSERVICE command could not be changed when the service was defined over a VLAN. This issue has been resolved.

PCR: 03294 Module: Alarm Level: 4

The port formatting for alarm messages was incorrect. This issue has been resolved.

PCR: 03296 Module: IPG Level: 2

Broadcast TCP packets were being processed by the device, causing fatal errors when firewall SMTP Proxy was configured. Non-unicast TCP packets are now dropped by IP.

PCR: 03298 Module: FIREWALL Level: 3

The SHOW FIREWALL POLICY was not showing the correct debugging items, as set with the ENABLE FIREWALL POLICY DEBUG command. This issue has been resolved.

PCR: 03300 Module: FIREWALL Level: 3

Firewall rules were not being applied to broadcast packets received on a public interface. This issue has been resolved.

PCR: 03305 Module: CORE, SWI Level: 4

On the SwitchBlade, the SHOW SYSTEM command was not displaying the PSU, fan tray, and fan status. This issue has been resolved.

PCR: 03311 Module: SWI Level: 2

If the ADD SWITCH FILTER command was used to add a static filter entry for a specific MAC address, and the ACTION parameter was set to FORWARD, then a packet sent to this address from another switch port would result in packet flooding on other link cards.

PCR: 03316 Module: CORE Level: 2

AT 9800 Series switches were not sending a temperature trap when the temperature exceeded the threshold of 40 °C. This issue has been resolved.

PCR: 03317 Module: OSPF Level: 2

Enabling OSPF via the GUI was sometimes causing fatal errors. This issue has been resolved.

PCR: 03318 Module: UTILITY Level: 2

When commands specified the notation, *line card.port number*, port numbers greater than the theoretical maximum of 256 were handled incorrectly. This issue has been resolved.

PCR: 03321 Module: DHCP, Q931, TELNET Level: 4

Debugging for DHCP and Q931 was not being disabled when a Telnet session finished. This issue has been resolved.

PCR: 03325 Module: IPG Level: 3

Illegal memory access problems were not producing diagnostic exception reports (stack dumps). This issue has been resolved.

PCR: 03327 Module: I750 Level: 3

The console was locking up under certain rare fault conditions. This issue has been resolved.

PCR: 03329 Module: IPG Level: 2

Each new entry into the IP routing table resulted in an ARP request being sent to resolve the next hop address. To prevent ARP flooding, a limit of 6 simultaneous ARP requests are transmitted.

PCR: 03331 Module: SWI, VLAN Level: 2

Changing a port's VLAN tagging was not updating the L3 multicasting entries for that port. This issue has been resolved.

PCR: 03332 Module: TTY Level: 4

A log message is now created when a user is forced to logout from an asynchronous port when another user (i.e. someone connected via Telnet) resets the asynchronous connection with the RESET ASYN command.

PCR: 03333 Module: IPG Level: 3

After VRRP was enabled, the link status of the switch ports was shown as UP, even if there was no connection to the ports. This issue has been resolved.

PCR: 03341 Module: STP Level: 3

STP ignores some BPDU packets coming in on tagged ports. This issue has been resolved. Now the VLAN tag is ignored on all devices except Rapier i Series Switches with multiple STPs on the receiving port.

PCR: 03342 Module: IPV6 Level: 3

Multicast Listener Discovery (MLD) was not setting the filter mode correctly when receiving certain packet types whilst in EXCLUDE mode. This issue has been resolved.

PCR: 03343 Module: UTILITY Level: 4

Entering a “?” on the command line, now displays the correct list of available options.

PCR: 03345 Module: IPG Level: 4

The RESET IP COUNTER=ALL command was not working correctly when issued from the command line. This issue has been resolved.

PCR: 03346 Module: SNMP Level: 4

Sometimes the *Agent Address* field in SNMP traps was not the same as the IP source address. This meant that sometimes the NMS did not send an alarm to the network manager when traps were received from switches. This issue has been resolved.

PCR: 03349 Module: BGP Level: 3

When there were a large number of BGP routes, the SHOW BGP ROUTE command sometimes caused an error. This issue has been resolved.

PCR: 03352 Module: PPP Level: 3

The MRU parameter in the SET PPP command was incorrectly handled as an interface parameter when the configuration script was generated. This meant that the OVER parameter was omitted. The MRU parameter is now correctly handled as a link parameter.

Features in SB251-11

Patch SB251-11 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:



After loading this software version, please check your alarm relay connections. Refer to PCR 03209 for more information.

PCR: 02331 Module: IPG, ETH Level: 2

IP is now informed when an Ethernet interface goes up or down, after a 2.5 second delay.

PCR: 02525 Module: TELNET, PING, IPV6, TCP Level: 3

The ADD IPV6 command was not allowing the INTERFACE parameter to be used when adding a host with link local address. This issue has been resolved.

PCR: 02571 Module: IP Level: 3

A fatal error occurred if the IP module was reset after the ADD IP EGP command was executed. This issue has been resolved.

PCR: 02577 Module: IPG, LOG Level: 4

The ability to log MAC addresses whenever the ARP cache changes has been added. To enable this, use the command:

```
ENABLE IP ARP LOG
```

To disable it, use the command:

```
DISABLE IP ARP LOG
```

The logging of MAC addresses is disabled by default. Use the SHOW LOG command to view the MAC addresses that have been logged when the ARP cache changes.

PCR: 02583 Module: FIREWALL Level: 2

UDP packets passed through the firewall by a reverse enhanced NAT rule were getting an incorrect IP checksum. This caused IP to discard the packets. This issue has been resolved.

PCR: 03032 Module: SWI Level: 3

If the ENABLE IP IGMP command was executed before the ENABLE SWITCH L3FILTER command, Layer 3 filtering did not discard packets destined for the CPU. This issue has been resolved.

PCR: 03035 Module: OSPF Level: 3

Erroneous Link State Advertisements (LSA's) were being sent whenever the Designated Router was removed from the network. This issue has been resolved.

PCR: 03044 Module: BGP Level: 2

During route flapping, peers were sometimes not told about routes to the same destinations as the flapping routes. This issue has been resolved.

PCR: 03059 Module: FIREWALL Level: 3

SMTP proxy was falsely detecting third party relay under some circumstances. This issue has been resolved.

PCR: 03062 Module: SWI Level: 4

Previously, *Get* or *GetNext* port state information could not be obtained from the *dot1dTpPortTable* and the *dot1dStpPortTable*. This issue has been resolved.

PCR: 03067 Module: DHCP Level: 1

When replying to a DHCP REQUEST that had passed through a DHCP relay, the broadcast bit of DHCP NAK messages was not being set. This issue has been resolved in accordance with RFC2131.

PCR: 03070 Module: BGP Level: 2

When BGP imported other route types, it would advertise routes that had next hops of the BGP peers themselves. The BGP peers would reject these routes and close the peering session, thus preventing the exchange of routing information between BGP peers. This issue has been resolved.

PCR: 03072 Module: BGP Level: 4

The Import parameter of the ADD, SET, DELETE and SHOW BGP commands now has an INTERFACE type. INTERFACE routes were previously grouped with STATIC routes.

PCR: 03078 Module: SWI,VLAN Level: 3:

DVMRP unicast *Prune*, *Graft*, and *Graft-Ack* messages are now switched at Layer 2.

PCR: 03078 **Module: SWI, VLAN** **Level: 3**

DVRMP messages *Prune*, *Graft* and *Graft-Ack* are now switched at Layer 2.

PCR: 03091 **Module: SWI** **Level: 4**

L2/L3/L4 hashing (used to allocate ports within a trunk group) was incorrectly formatted. This issue has been resolved.

PCR: 03095 **Module: DHCP** **Level: 2**

DHCP policies are no longer stored in alphabetical order in the DYNAMIC CONFIGURATION script because this did not work when the DHCP INHERIT parameter was used.

PCR: 03111 **Module: FIREWALL** **Level: 1**

TCP sessions could fail if the public side of the firewall was using Kerberos and the private side had a very slow connection to the firewall. This issue has been resolved.

PCR: 03116 **Module: FIREWALL** **Level: 2**

An error sometimes occurred in the firewall module under heavy FTP or RTSP traffic loads. This issue has been resolved.

PCR: 03120 **Module: ETH, IPG** **Level: 4**

The SHOW IP INTERFACE command was showing ETH interfaces as up at startup, when SHOW INTERFACE and SHOW ETH STATE had them as down. This issue has been resolved.

PCR: 03124 **Module: IPV6** **Level: 4**

The SHOW IPv6 COUNTER command now shows the *outAdvert* messages in the Total Out Messages counter field.

PCR: 03126 **Module: DHCP** **Level: 2**

DHCP assigned incorrect IP addresses to clients shifting from a relayed to a non-relayed range. This issue has been resolved.

PCR: 03139 **Module: IPV6** **Level: 3**

The SHOW IPV6 INTERFACE command was not displaying the link layer address and EUI when the interface was down. This issue has been resolved.

PCR: 03144 **Module: CURE** **Level: 4**

Users with either USER or MANAGER level privilege can now execute the STOP PING and STOP TRACE commands. Previously, MANAGER privilege was needed to execute these commands.

PCR: 03145 **Module: IPG** **Level: 4**

The SET IP ROUTE FILTER command was not processing some parameters. This issue has been resolved.

PCR: 03146 Module: PORT Level: 4

The PAGE parameter in the SET ASYN command now only accepts numeric values between 0 and 99, ON or OFF, and TRUE or FALSE.

PCR: 03147 Module: BGP Level: 4

When the DISABLE BGP DEBUG command was used, debugging messages were still being displayed by the BGP module. This issue has been resolved.

PCR: 03150 Module: FIREWALL Level: 4

The CREATE FIREWALL POLICY command was not checking for valid name entries, so invalid printing characters could be used for policy names. This issue has been resolved.

PCR: 03152 Module: IPG Level: 4

An additional check has been added to validate the MASK specified in an ADD IP ROUTE command. The check tests that the mask is contiguous.

PCR: 03155 Module: FFS Level: 4

The SHOW FFILE command output has changed. The first column that listed where the file was stored has been removed. The title of the original second column (now the first column) has been changed from "creator" to "module". The file format specifier has been altered from:

```
DDDD:MMMM\NNNNNNNNN.TTT
```

to:

```
MMMM\NNNNNNNNN.TTT
```

PCR: 03163 Module: IPG Level: 3

IGMP Snooping did not use DVMRP messages to identify a port. This issue has been resolved.

PCR: 03166 Module: IPG Level: 4

The output of the SHOW IP IGMP COUNTER and SHOW IGMP SNOOPING COUNTER commands was incorrect. This issue has been resolved.

PCR: 03167 Module: DVMRP Level: 2

When multicasting to a VLAN interface, if more than 2 DVMRP neighbours existed on a single port, and any one of those neighbours was pruned, the multicast data would stop flowing to the port. This happened even though it was still required for the remaining DVMRP neighbours. This issue has been resolved.

PCR: 03169 Module: IPV6 Level: 2

Duplicate Address Detection (DAD) was not sent on VLAN interfaces. This issue has been resolved.

PCR: 03172 Module: FIREWALL Level: 2

Telnet access was not being denied when used between public interfaces. This issue has been resolved.

PCR: 03178 **Module: IPSEC** **Level: 4**

An unnecessary check has been removed from the CREATE ISAKMP POLICY AUTHTYPE=RSASIG command.

PCR: 03185 **Module: DHCP** **Level: 2**

A Switchblade configured as a DHCP client could not receive unicast messages. To resolve this issue, the Switchblade will now request that the server responds by using broadcast messages.

PCR: 03186 **Module: CORE, FFS, TTY** **Level: 4**

When the QUIT option was chosen after the SHOW DEBUG command was executed, the output did not immediately stop. This issue has been resolved, but there may be a short delay before the command prompt reappears.

PCR: 03188 **Module: IPG, SWI, VRRP** **Level: 3**

For switches configured for VRRP, it was not possible to Ping the switch operating in the Master state. This issue has been resolved.

PCR: 03189 **Module: FIREWALL, LB** **Level: 3**

A fatal error occurred in the load balancer when there were no UP resources in a resource pool. This issue has been resolved. Load balanced TCP connections will now only retry SYNs once after 5 seconds. The round robin selection algorithm will now select an UP resource in a resource pool with only one UP resource, even if it was used for the last successful connection.

PCR: 03194 **Module: LB** **Level: 3**

Sometimes healthcheck pings were not sent to the load balancer resources. This issue has been resolved.

PCR: 03196 **Module: IPV6** **Level: 3**

The system became unstable if the ADD IPV6 TUNNEL command failed. This instability was caused by the partially created tunnel entry not being properly removed from the tunnel database. The tunnel entry is now completely removed.

PCR: 03199 **Module: IPV6** **Level:**

Invalid routes and packets were occurring within RIP. This issue has been resolved.

PCR: 03201 **Module: SWI** **Level: 4**

AT-9800 Series switches with 16 ports could be configured beyond their 16 port maximum. Attempting to configure port 17 would produce no error message, and attempting to configure ports 18 and above would result in an incorrect error message. Also, the SwitchBlade could be allocated with 17 ports within a single trunk group, one port more than the maximum. These issues have been resolved; in both instances the maximum port configuration is now 16.

PCR: 03203 Module: IPV6 Level: 3

RIPng was not sending a response back to a RIP request message. This issue has been resolved.

PCR: 03206 Module: IPG Level: 3

IPv4 filters now behave like IPv6 filters.

PCR: 03208 Module: FIREWALL Level: 2

When the configuration script was created using the CREATE CONFIG command, the GBLIP parameter in the ADD FIREWALL POLICY command was listed twice. This caused the command to fail when the device was restarted. This issue has been resolved.

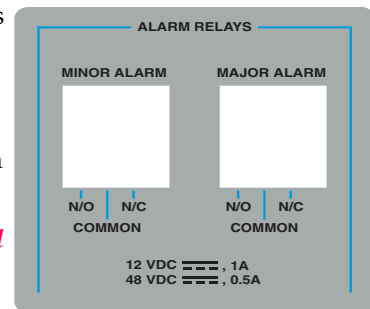
PCR: 03209 MODULE: ALARM Level: 1

The action of the MAJOR and MINOR relays does not presently match the illustration located alongside their connections.

This issue has been resolved by reversing the action of the relays in software to match the illustration shown on the right.



Please check that your alarm relays are still appropriately connected.



PCR: 03210 Module: PING Level: 4

The SET TRACE PORT command was not functioning correctly. Also, the SHOW CONFIG DYNAMIC PING command was producing an incorrect output format. These issues have been resolved.

PCR: 03212 Module: IPV6 Level: 3

The TRACE command was not working when using an IPv6 link-local address. This issue has been resolved.

PCR: 03213 Module: IPSEC Level: 3

A memory leak occurred when some IPSEC processes failed. This issue has been resolved.

PCR: 03214 Module: PIM Level: 2

Parallel forwarding PIM neighbours were not always sending PIM *Assert* messages following a neighbour re-boot. This was causing the transmission of duplicate multicast data. This issue has been resolved.

PCR: 03216 Module: PIM, PIM6 Level: 2

PIM4 and PIM6 were not sending *Hello* packets if the HELLOINTERVAL was not a multiple of 10. This is set with the ADD PIM INTERFACE, ADD PIM6 INTERFACE, SET PIM INTERFACE, and SET PIM6 INTERFACE commands. This issue has been resolved.

PCR: 03217 Module: DVMRP Level: 2

If a DVMRP interface was deleted and then added again, DVMRP routes associated with this interface were not reactivated. This issue has been resolved.

PCR: 03222 Module: PIM, PIM6 Level: 2

If the RP candidate advertising time was set to a non-default value with the ADVINTERVAL parameter in the SET PIM command, the hold time in the message was not being updated correctly. This issue has been resolved.

PCR: 03223 Module: SWI Level: 2

The output from the SHOW SWITCH PORT COUNTER command was showing incorrect values for packets greater than 1519 bytes. This issue has been resolved.

PCR: 03224 Module: IPG Level: 2

If an IP address was added using the AD IP INTERFACE IP=DHCP and the server could not assign an IP address due to a network problem affecting the server's VLAN, any further frames transmitted to IP addresses on other VLANS would be blocked. This issue has been resolved.

PCR: 03227 Module: SWI Level: 4

Previously, the default output of the SHOW SWITCH FDB command displayed the forwarding database information for ports on the controller card located in bay A. The default now displays all external ports for switch instances except for those on the controller card. This command no longer displays information about internal ports.

PCR: 03229 Module: LOAD Level: 3

Zmodem was not naming some loaded files. This issue has been resolved.

PCR: 032231 STP Level: 3

STP was advertising an incorrect length for BPDU packets. This issue has been resolved.

PCR: 03232 Module: BGP Level: 3

Values for the KEEPALIVE and HOLDDTIME parameters in the ADD BGP PEER and SET BGP PEER commands were not interacting correctly. This issue has been resolved.

PCR: 03234 Module: IPG Level: 3

The PURGE IP command did not remove ENABLE IP IGMP from the configuration. This issue has been resolved.

PCR: 03236 Module: IPG Level: 3

IGMP queries were being sent after IGMP was disabled. This issue has been resolved.

PCR: 03237 Module: IPG Level: 2

RIP *Request* packets for IPv4 were not being transmitted when the link came up or when the switch restarted. This issue has been resolved.

PCR: 03238 Module: SWI Level: 2

When RIP interfaces were deleted, the IP routes learned through those interfaces were not timing out correctly. Now, all IP routes learned through a RIP interface are removed when the RIP interface is deleted, and no timeouts occur.

PCR: 03239 Module: QOS Level: 2

QoS Traffic Class maximum bandwidth limiting was being overwritten by the port or trunk maximum bandwidth value. This should only happen when the Traffic Class maximum bandwidth has *not* been set manually with the CREATE QOS TRAFFICCLASS MAXBANDWIDTH parameter. This issue has been resolved.

PCR: 03240 Module: OSPF Level: 2

A fatal error occurred when OSPF was under high load. This issue has been resolved.

PCR: 03244 Module: ETH, IPG Level: 3

ARP table entries are now deleted when an ETH interface goes down.

PCR: 03245 Module: SWI, IPG, PIM Level: 2

Multicast streams would not commence forwarding immediately due to IGMP packets initiated but not sent while a VLAN was changing from the DOWN to UP state. Also, multicast streams could be received while the VLAN was changing from DOWN to UP, causing a PIM Reverse Path Forwarding unicast route lookup failure. This was due to the unicast route being unusable as the VLAN was still considered down. These issues have been resolved.

PCR: 03246 Module: SWI Level: 3

For the SwitchBlade and AT-9800 Series Switches, the TTL egress limit for forwarding IP multicast packets has been increased from 0 to 1. Therefore, only packets with a TTL greater than 1 will be forwarded.

PCR: 03248 Module: VLAN Level: 4

The error message for an incorrectly added or removed port now displays both the card and the port identifiers.

PCR: 03250 Module: SWI Level: 4

The DELETE SWITCH FILTER command did not work properly when the ENTRY parameter was assigned a range with hyphen ("-"). This issue has been resolved.

PCR: 03252 Module: PIM Level: 3

An assert storm sometimes occurred with PIM-DM. This issue has been resolved.

PCR: 03254 Module: BGP Level: 2

If, with one or more routes already configured, BGP was enabled and an additional route added, BGP was not aggregating the new route. This issue has been resolved.

PCR: 03256 Module: MLD Level: 3

MLD did not respond correctly when it was in *exclude* mode and it received a request block. This issue has been resolved.

PCR: 03257 Module: SWI Level: 2

When using the SET SWITCH PORT command, setting port intrusion caused static MAC addresses to be deleted. This issue has now been resolved.

PCR: 03260 Module: SWI, SNMP Level: 4

The SNMP MIB browser was returning nonaligned pairs following a *GetNext* of the FDB table. This issue has been resolved.

PCR: 03261 Module: VLAN, IPG Level: 4

VLAN and IPG packet debugging facility has now been restored.

PCR: 03262 Module: PPP Level: 3

The CREATE CONFIGURATION command adds the PPP TEMPLATE LQR parameter when LQR is enabled. But the configuration script always contained "LQR=ON" even when the LQR value was not the default. This issue has been resolved.

PCR: 03263 Module: SWI Level: 4

The EGRESS parameter setting was not displayed by the SHOW CONFIG DYNAMIC command. This issue has been resolved.

PCR: 03265 Module: SWI Level: 3

The IFHC counter used within the SNMP MIB was producing incorrect counts. This issue has been resolved.

PCR: 03266 Module: PIM Level: 2

The handling of the upstream neighbour for a *GraftACK* message has been corrected.

PCR: 03273 Module: ALARM Level: 4

The PORT parameter of the ADD ALARM command would not accept a range of ports. This issue has been resolved.

PCR: 03274 Module: SWI Level: 4

Entering the command, SET SWITCH TRUNK SPEED was returning the inappropriate error message, "The INSTANCE specified does not exist." This issue has been resolved.

PCR: 03275 Module: SWI Level: 2

On SwitchBlade and AT-9800 Series switches, adding a static ARP entry resulted in the entry of the MAC address being added for the next hop port. These addresses were being incorrectly added if the next hop port was configured as a tagged port. This issue has been resolved.

PCR: 03278 Module: IPV6 Level: 4

The timing of LLQ packets has been modified to be consistent with MLD Draft (Nov 2002).

PCR: 03280 Module: IPG, BGP Level: 1

BGP/IPG was causing fatal errors to occur following network topology changes. This issue has been resolved.

PCR: 03284 Module: SWI Level: 4

Setting addresses using the SET SWITCH BLADE IP command resulted in the SHOW SWITCH TAB=IP command displaying incorrect addresses.

PCR: 03285 Module: IPG Level: 4

RIP packets can now contain up to 25 routes per packet instead of 24.

PCR: 03288 Module: L2TP Level: 2

When a radius lookup performed by the L2TP Access Concentrator (LAC) failed, the LAC attempted to disconnect the call from its tunnel. If the tunnel had not been created, the device restarted. This issue has been resolved.

PCR: 03290 Module: SWI Level: 2

PINGING between blades within the same switch failed whenever the current master was located in the right-hand slot and a control blade was located in the left-hand slot. This issue has been resolved.

PCR: 03291 Module: PPP Level: 2

A PAP authentication failure with PPPoE could cause a fatal error. This issue has been resolved.

PCR: 03293 Module: PPP Level: 3

The MAXSESSION parameter of the SET PPP ACSERVICE command could not be changed when the service was defined over a VLAN. This issue has been resolved.

PCR: 03294 Module: Alarm Level: 4

The port formatting for alarm messages was incorrect. This issue has been resolved.

PCR: 03295 Module: IP Level: 2

Static IP ARP entries were not being written to the hardware table. This issue has been resolved.

PCR: 03296 Module: IPG Level: 2

Broadcast TCP packets were being processed by the device, causing fatal errors when firewall SMTP Proxy was configured. Non-unicast TCP packets are now dropped by IP.

PCR: 03298 Module: FIREWALL Level: 3

The SHOW FIREWALL POLICY was not showing the correct debugging items, as set with the ENABLE FIREWALL POLICY DEBUG command. This issue has been resolved.

PCR: 03300 Module: FIREWALL Level: 3

Firewall rules were not being applied to broadcast packets received on a public interface. This issue has been resolved.

PCR: 03305 Module: CORE, SWI Level: 4

On the SwitchBlade, the SHOW SYSTEM command was not displaying the PSU, fan tray, and fan status. This issue has been resolved.

PCR: 03311 Module: SWI Level: 2

If the ADD SWITCH FILTER command was used to add a static filter entry for a specific MAC address, and the ACTION parameter was set to FORWARD, then a packet sent to this address from another switch port would result in packet flooding on other link cards.

PCR: 03316 Module: CORE Level: 2

AT 9800 Series switches were not sending a temperature trap when the temperature exceeded the threshold of 40 °C. This issue has been resolved.

PCR: 03317 Module: OSPF Level: 2

Enabling OSPF via the GUI was sometimes causing fatal errors. This issue has been resolved.

PCR: 03318 Module: UTILITY Level: 2

When commands specified the notation, *line card.port number*, port numbers greater than the theoretical maximum of 256 were handled incorrectly. This issue has been resolved.

PCR: 03321 Module: DHCP, Q931, TELNET Level: 4

Debugging for DHCP and Q931 was not being disabled when a Telnet session finished. This issue has been resolved.

PCR: 03325 Module: IPG Level: 3

Illegal memory access problems were not producing diagnostic exception reports (stack dumps). This issue has been resolved.

PCR: 03327 Module: I750 Level: 3

The console was locking up under certain rare fault conditions. This issue has been resolved.

PCR: 03329 Module: IPG Level: 2

Each new entry into the IP routing table resulted in an ARP request being sent to resolve the next hop address. To prevent ARP flooding, a limit of 6 simultaneous ARP requests are transmitted.

PCR: 03331 Module: SWI, VLAN Level: 2

Changing a port's VLAN tagging was not updating the L3 multicasting entries for that port. This issue has been resolved.

PCR: 03332 Module: TTY Level: 4

A log message is now created when a user is forced to logout from an asynchronous port when another user (i.e. someone connected via Telnet) resets the asynchronous connection with the RESET ASYN command.

PCR: 03333 Module: IPG Level: 3

After VRRP was enabled, the link status of the switch ports was shown as UP, even if there was no connection to the ports. This issue has been resolved.

PCR: 03335 Module: SWI Level: 2

Broadcast storm control (BCSC) rate limiting was not operating on broadcast packets when set per VLAN. This issue has been resolved.

PCR: 03341 Module: STP Level: 3

STP ignores some BPDU packets coming in on tagged ports. This issue has been resolved. Now the VLAN tag is ignored on all devices except Rapiet i Series Switches with multiple STPs on the receiving port.

PCR: 03342 Module: IPV6 Level: 3

Multicast Listener Discovery (MLD) was not setting the filter mode correctly when receiving certain packet types whilst in EXCLUDE mode. This issue has been resolved.

PCR: 03343 Module: UTILITY Level: 4

Entering a "?" on the command line, now displays the correct list of available options.

PCR: 03345 Module: IPG Level: 4

The RESET IP COUNTER=ALL command was not working correctly when issued from the command line. This issue has been resolved.

PCR: 03346 Module: SNMP Level: 4

Sometimes the *Agent Address* field in SNMP traps was not the same as the IP source address. This meant that sometimes the NMS did not send an alarm to the network manager when traps were received from switches. This issue has been resolved.

PCR: 03349 Module: BGP Level: 3

When there were a large number of BGP routes, the SHOW BGP ROUTE command sometimes caused an error. This issue has been resolved.

PCR: 03352 Module: PPP Level: 3

The MRU parameter in the SET PPP command was incorrectly handled as an interface parameter when the configuration script was generated. This meant that the OVER parameter was omitted. The MRU parameter is now correctly handled as a link parameter.

PCR: 03353 Module: PPP Level: 3

Dynamic interface details were added through the SET INTERFACE command when the CREATE CONFIGURATION command was executed. This caused errors on startup. This issue has been resolved.

PCR: 03354 Module: Firewall Level: 4

The command SET FIREWALL POLICY RULE BEFORE=24:00, which was used to set a rule back to its default of "until midnight," was found to be failing. This issue has been resolved.

PCR: 03355 Module: IPV6 Level: 4

IPv6 over IPv4 tunnelling failed unless an IPv4 interface was configured. This issue has been resolved.

PCR: 03356 Module: SWI Level: 2

Deleting hardware filters on a SwitchBlade was producing fatal errors. This issue has been resolved.

PCR: 03359 Module: CORE Level: 3

An incorrect object ID (OID) was being returned for Fan/PSU in SNMP v1 trap messages. This issue has been resolved.

PCR: 03360 Module: STP Level: 4

Entering a ? after SET STP=*stp-name*, at the CLI, to request context-sensitive help, only returned the PORT and DEFAULT options. This issue has been resolved so that all options are now shown.

PCR: 03361 Module: SWI Level: 2

A fatal error was occurring on the SwitchBlade if restarting the switch coincided with full line speed transmission into a G8F line card. This issue has been resolved.

PCR: 03364 Module: PIM Level: 4

PIM will no longer accept obsolete commands.

PCR: 03369 Module: FIREWALL Level: 2

TCP checksums in TCP packets passing through the firewall were being recalculated incorrectly when the TCP setup proxy was disabled, and enhanced NAT was in use. This issue has been resolved.

PCR: 03371 Module: DHCP Level: 3

A minimum lease time can no longer be specified when creating a DHCP policy. This complies with RFC 2131.

PCR: 03374 Module: IPV6 Level: 1

Multilink Listener Discovery (MLD) packets received on the switch caused fatal errors. This issue has been resolved.

PCR: 03375 Module: IPG Level: 2

The following issues with IPv6 have been resolved:

- Incorrect default values were set for the PREFERRED and VALID parameters in the ADD IPV6 PREFIX command. The correct default for PREFERRED is 604800 seconds (7 days), and the correct default for VALID is 2592000 seconds (30 days).
- The PREFERRED and VALID parameters in the ADD IPV6 PREFIX and SET IPV6 PREFIX commands were accepting values that could make the preferred life time longer than the valid life time.
- The POISONREVERSE parameter in the ADD IPV6 RIP command was not added to the automatic configuration.

PCR: 03376 Module: SWI Level: 4

With the SET SWI PORT SPEED set to 1000MFULL for a GBIC port, the LINK LED was turning on with no GBIC installed. This issue has been resolved.

PCR: 03379 Module: IPSEC Level: 3

If IPsec was using PPPoE, the initiator continued to keep the IPsec SA even if the PPPoE session failed and the ISAKMP Heartbeat timer expired. This issue has been resolved.

PCR: 03382 Module: SWI Level: 2

A maximum of 63 ports can belong to a VLAN multicast group. When this figure was exceeded data ceased to flow to many of the ports. A resolution has been applied that allows the first 63 ports to continue receiving multicast data.

PCR: 03383 Module: IPG Level: 2

With large numbers of routes configured, entering the SHOW IP ROUTE command could produce a fatal error. This issue has been resolved.

PCR: 03384 Module: IPV6 Level: 3

Multicast Listener Discovery (MLD) packets were being transmitted with incorrect source lists, following the receipt of TO_EX(A) packets. This issue has been resolved.

PCR: 03387 Module: PIM, PIM6 Level: 2

A memory leak occurred in IP or IPV6 if PIM-SM received IGMP or MLD reports, and there was no Rendezvous Point for the reported group.

PCR: 03388 Module: DHCP Level: 3

The DHCP lease *Expiry* time showed incorrectly in the SHOW DHCP CLIENT command when the lease straddled across multiple months and years. This issue has been resolved.

PCR: 03390 Module: HTTP Level: 2

Occasionally a fatal error occurred when the GUI browser started or a page was refreshed. This issue has been resolved.

PCR: 03394 Module: OSI/CLNS Level: 1

A fatal error sometimes occurred if the SHOW CLNS ROUTE command was executed when a large number of routes had been learned. This issue has been resolved.

PCR: 03395 Module: BGP Level: 3

The time delay for BGP peers to back off following a transition from an ESTABLISHED to an IDLE state has been changed. Previously the delay grew exponentially and would never decay. It is now fixed at one second.

PCR: 03400 Module: SSL Level: 3

Under certain conditions, an incomplete SSL handshake, or a TCP packet sent with the FIN bit set but with no data Secure Sockets Layer (SSL), would not allow the TCP session to close properly. Also SSL would leak memory when it received SSL records. These issues have been resolved.

PCR: 03407 Module: IPG Level: 3

The default for the PROXYARP parameter in the SET IP INTERFACE command for a VLAN interface was OFF. The default is now ON.

PCR: 03412 Module: FIREWALL Level: 3

FTP data transfers did not succeed for some types of NAT. Also, the presence of flow control TCP flags meant that some TCP control packets were not recognised. These issues have been resolved.

PCR: 03413 Module: BGP Level: 2

The BGP route table was updated according to the most recently added route. BGP now updates to reflect the best available route, regardless of when it was added.

PCR: 03421 Module: IPG Level: 2

IP entries were not correctly updated when multiple logical IP interfaces existed on the same VLAN whenever there was a VLAN up or down state change. This issue has been resolved.

PCR: 03423 Module: IP Level: 4

The ADD IP ROUTE command allowed an incorrect mask to be set for the default route, i.e. to values other than 0.0.0.0. This issue has been resolved and now the only permitted mask value for the default route is 0.0.0.0.

PCR: 03424 Module: DHCP Level: 2

When static DHCP was set to the first IP address in a range, that range would stay in the *Reclaim* mode. This issue has been resolved.

PCR: 03426 Module: IPV6 Level: 3

If the valid and preferred lifetimes of an IPv6 address for a given interface were set to infinity, they were not included in the dynamic configuration. This issue has been resolved.

PCR: 03428 Module: STP Level: 3

In Rapid STP mode, ports did not always make rapid changes to the Forwarding State when their roles changed from Alternate to either Designated or Root. This issue has been resolved.

PCR: 03429 Module: SWI, VLAN Level: 3

The SHOW VLAN command displayed a nonexistent port. This issue has been resolved.

PCR: 03430 Module: BGP Level: 3

The BGP traps sent to either establish or lower its peer states were incorrectly set. This issue has been resolved.

PCR: 03432 Module: STP Level: 3

STP settings were not retained when a port was deleted from the VLAN that the STP belongs to. This issue has been resolved.

PCR: 03433 Module: CFLASH Level: 2

A fatal error would occur if the command SET CFLASH DIRECTORY was used to set a non-existent, or invalid directory. This issue has been resolved.

PCR: 03436 Module: IP, DHCP Level: 3

When the device was acting as a DHCP client and the DHCP server provided a gateway address, a statically configured default route was deleted and replaced with a default route with the provided gateway address. The correct behaviour is to only delete a dynamic default route in this situation. This issue has been resolved; the correct behaviour is now applied.

PCR: 03438 Module: DHCP Level: 3

A warning message will now appear if the DESTROY DHCP POLICY command is executed for a DHCP policy that has been used by one or more policies as the source of their configuration information. A parent policy can be destroyed with no affect on its child policies.

The new message is:

The destroyed policy <policy-name> has been used by another policy as a source of configuration information.

PCR: 03439 Module: IPX Level: 3

The IPX traffic filter match counter was not incremented if a route was cached. This issue has been resolved.

PCR: 03441 Module: L2TP Level: 2

PPP configured on a L2TP access concentrator (LAC) should be dynamic. If PPP was incorrectly configured to be static, the static PPP was destroyed when the L2TP tunnel was formed so that only the first connection succeeded. This issue has been resolved so that an L2TP tunnel is not created if the PPP is static.

PCR: 03443 Module: DHCP Level: 3

When a DHCP entry expired while other DHCP entries in the range were in *Reclaim* mode, unnecessary ARP packets were generated causing an ARP storm. This issue has been resolved.

PCR: 03447 Module: PPP Level: 2

A remotely assigned IP address on a PPP interface was not always released when the connection timed out. This issue has been resolved.

PCR: 03448 SWI Level: 4

The output from the SHOW SWI FDB command now includes the total number of entries displayed.

PCR: 03450 PIM, PIM6 Level: 3

Receiving PIM State *Refresh* messages will now either create or maintain PIM (S,G).

PCR: 03453 FIREWALL Level: 4

The Dropped Packets counter was not incrementing correctly. This issue has been resolved.

PCR: 03454 IPV6 Level: 2

In rare circumstances, removing the cable from an IPv6 interface was resulting in fatal errors. This issue has been resolved.

PCR: 03456 Module: PIM Level: 2

A VLAN interface receiving a PIM *Prune* message on a port stopped forwarding multicast data to that port too early. This could cause multicast data to arrive after a PIM *Prune*, so an override PIM *Join* message was not sent, leading to a loss of multicast data. This issue has been resolved.

PCR: 03457 Module: OSPF Level: 2

Disabling OSPF caused a fatal error if there was a large routing table. This issue has been resolved.

PCR: 03459 Module: IPV6 Level: 2

A fatal error could occur if IPv6 flows were disabled while packets were being forwarded via an IPv6 interface. This issue has been resolved.

PCR: 03460 Module: PIM4 Level: 3

PIM-DM was delaying *Assert* messages after a prune hold time expired. This issue has been resolved.

PCR: 03462 **Module: PIM, PIM6** **Level: 3**

PIM *Graft* and *Graft-Ack* counters were not incrementing. This issue has been resolved.

PCR: 03464 **Module: PIM, PIM6** **Level: 3**

PIM-SM *Null* register messages for non-PIM-SM domain sources did not have the *Border* bit set. This issue has been resolved.

PCR: 03465 **Module: DHCP** **Level: 3**

The IPMTU parameter in the ADD DHCP POLICY command was accepting values in the range 0-4294967295. This parameter now accepts values in the correct range of 579-65535.

PCR: 03467 **Module: IPG** **Level: 3**

An invalid message appeared when the PORT parameter was specified for the ADD IP ROUTE command. This issue has been resolved.

PCR: 03468 **Module: PIM** **Level: 3**

The source IP address in a PIM *Register* message was not the DR interface's IP address. This issue has been resolved.

PCR: 03469 **Module: CORE** **Level: 3**

Secure mode was being disabled after a re-boot. Secure mode should only be disabled by executing the DISABLE SYSTEM SECURITY command. This issue has been resolved.

PCR: 03471 **Module: IPV6** **Level: 2**

A fatal error sometimes occurred when forwarding traffic over an IPv6 tunnel. This issue has been resolved.

PCR: 03474 **Module: FIREWALL** **Level: 3**

The SMTP proxy did not correctly allow outgoing (private to public) SMTP sessions when the DIRECTION parameter was set to OUT or BOTH in the ADD FIREWALL PROXY command. This issue has been resolved.

PCR: 03475 **Module: NTP** **Level: 3**

The PURGE NTP command did not change the UTC offset to the initialised

PCR: 03476 **Module: IPV6** **Level: 3**

RIPng was showing routes to interfaces that were DOWN as being UP. This issue has been resolved.

PCR: 03478 **Module: PIM, PIM6** **Level: 3**

The message format for PIM-SM periodic (*,*,RP) *Join* messages was incorrect when the message contained more than one joined RP address. This issue has been resolved.

PCR: 03479 Module: SWI Level: 3

Typing "?" for Help at the CLI for the SHOW SWITCH FDB command displayed some invalid parameters, and the valid STATUS parameter was not displayed. This issue has been resolved.

PCR: 03483 Module: SWI Level: 3

The commands ADD SWITCH BLADE and DELETE SWITCH BLADE have been disabled because they initiate internal SwitchBlade processes.

PCR: 03484 Module: FIREWALL Level: 2

The firewall was not denying an ICMP packet, even if ICMP Forwarding was disabled when using Standard NAT. This issue has been resolved.

PCR: 03485 Module: CFLASH Level: 2

On AT-9800 Series switches, the current directory for CompactFlash changed when it should not have. This issue has been resolved.

PCR: 03489 Module: SYSR Level: 2

The feature licence mismatch message was not showing when the master has no feature licence, and the slave does. This issue has been resolved.

PCR: 03490 Module: IPSEC Level: 2

IPSec used with IPv4 sometimes caused a fatal error. This issue has been resolved.

PCR: 03492 Module: HTTP, LOAD Level: 3

Some memory loss occurred when loading a file via HTTP. This issue has been resolved.

PCR: 03494 Module: BGP, FIREWALL Level: 2

If the firewall was enabled when BGP was in use, outgoing BGP data packets would have IP header errors and incorrect checksums. This problem has been resolved.

PCR: 03497 Module: PIM, PIM6 Level: 2

If, in a network comprising alternative paths, a link connecting to a Candidate Rendezvous Point (CRP) was down, the CRP would not re-advertise its RP candidacy on other paths. The switch would therefore not update its PIM routes and re-establish the PIM tree in order for multicast data to flow again. This issue has been resolved.

PCR: 03499 Module: IPG Level: 2

The SET TIME command caused an error on *Refresh* timers for IGMP groups. This issue has been resolved.

PCR: 03502 Module: IPG Level: 3

The ENTRY parameter of the ADD IP FILTER command was not included in the output of the SHOW CONFIG DYNAMIC command. This issue has been resolved.

PCR: 03511 Module: IPG Level: 3

The special group entry 01-00-5e-00-00-02 was being written to the layer 2 forwarding database to identify router ports for IGMP snooping. Router ports are now identified from software, so this special group entry is no longer written to the layer 2 forwarding database.

PCR: 03514 Module: IPSEC Level: 2

An incorrect IPSec Security Association (SA) was used to transmit packets when the SA's IP address was assigned dynamically on another VPN gateway. This issue has been resolved.

PCR: 03515 Module: DHCP Level: 3

DHCP was offering network and broadcast addresses to clients. This issue has been resolved.

PCR: 03516 Module: SWI Level: 3

Continuous messages associated with CAM are sometimes generated on SwitchBlade series switches. If this happens, please contact your authorised distributor or reseller so that this issue can be resolved. The messages are similar to the following:

```
swiCXeVirtCamTranslateAddress - ulEntryNo:4294967254
entries:8192 last:106495.
```

PCR: 03517 Module: FIREWALL Level: 3

An error was not returned if the SET FIREWALL POLICY RULE command was executed with PROTOCOL=1 when ICMP forwarding was turned on. This issue has been resolved so that an error is now displayed.

PCR: 03522 Module: IKMP Level: 3

ISAKMP suffered an error when it encountered unknown cryptographic algorithms. This issue has been resolved.

PCR: 03523 Module: FIREWALL Level: 2

In some circumstances the checksum for the TCP header was set to zero. This issue has been resolved.

PCR: 03526 Module: SWI Level: 3

The Switch MIB did not show the correct *dot1StpPriority* value. This issue has been resolved.

PCR: 03527 Module: BGP Level: 4

Session-only counters have been added to the MIB entry for BGP peers.

PCR: 03532 Module: FIREWALL Level: 2

Occasionally the TCP connection was terminated early during an IDENT proxy TCP session. This issue has been resolved.

PCR: 03533 Module: PIM Level: 3

A forwarded PIM-DM state *Refresh* message did not update the metric and preference values. This issue has been resolved.

**PCR: 03534 Module: ALARM, CFLASH,
CORE, DIAG, DUART, FFS, GUI,
HTTP, LOAD, M8240, MONITOR Level: 3**

Added support for the new AT-9816GB-DC, and 9812T-DC hardware.

PCR: 03535 Module: IPG Level: 2

IGMP *Query* messages were not sent after IGMP was disabled and then re-enabled. This issue has been resolved.

PCR: 03536 Module: BGP, TCP Level: 3

Outgoing BGP packets did not have the Internet Work control flags set in the IP TOS bits. This issue has been resolved.

PCR: 03537 Module: BGP Level: 3

BGP was returning incorrect and/or incomplete *bgp4AttrPath* MIB entry information. This issue has been resolved.

PCR: 03538 Module: BGP Level: 3

Configuration information was not exported to BGP peers when BGP was disabled and then re-enabled. This issue has been resolved.

PCR: 03539 Module: IPG, BGP Level: 2

Some packets sent from BGP had an incorrect source IP address because it was set to the IP address of the interface that was configured first. This issue has been resolved. Packets are now always sent with the correct source IP address.

PCR: 03543 Module: IPG Level: 1

When the device was acting as a DNS relay agent, a fatal error occurred after approximately 3 hours of heavy load. This issue has been resolved.

PCR: 03544 Module: HTTP, FIREWALL Level: 3

HTTP proxy was not denying an IP address if its corresponding domain name was specified in a filter, or if a domain name was requested and its corresponding IP address was in the filter. This issue has been resolved.

PCR: 03547 Module: DHCP Level: 3

The range of values for the IPMTU parameter in the ADD DHCP POLICY command was set incorrectly in PCR 03465. The correct range is 576-65535, not 579-65535. This issue has been resolved.

PCR: 03549 Module: IPV6 Level: 3

IPv6 filters were not working correctly when the last entry of a filter was altered using the SET IPV6 FILTER command. This issue has been resolved

PCR: 03551 Module: IPV6 Level: 2

The command ADD IPV6 6TO4 IP did not allow more than one tunnel. This issue has been resolved. This command can now be used repeatedly to create multiple tunnels.

PCR: 03555 Module: HTTP Level: 3

The RESET HTTP SERVER command was resetting the dynamic configuration settings back to the default values. This command now resets the HTTP server counters, and restarts the HTTP server using the dynamic configuration settings.

PCR: 03558 Module: PIM, PIM6 Level: 2

Periodic PIM (*,*,RP) *Join* messages did not cease after a set Rendezvous Point timed out. This issue has been resolved.

PCR: 03560 Module: IPV6 Level: 2

A fatal error sometimes occurred when IPv6 multicast packets were forwarded via an interface that went down and then came back up. This issue has been resolved.

PCR: 03561 Module: CORE Level: 3

To reduce the number of necessary high temperature indications, the temperature warning threshold on the AT-9800 Series Switch has been increased from 40 °C to 60 °C.

PCR: 03562 Module: IPV6 Level: 3

Disabling and then enabling IPv6 made the CREATE IPV6 INTERFACE=VLAN command appear twice in the configuration script. This issue has been resolved.

PCR: 03564 Module: IPV6 Level: 2

A fatal error sometimes occurred when an IPv6 flow used a virtual interface, and the flow was displayed using the SHOW IPV6 FLOW command. This issue has been resolved.

PCR: 03565 Module: BGP Level: 2

A fatal error occurred after executing the SET BGP PEER command when a BGP session was established with more than 15 communities defined. This issue has been resolved.

PCR: 03566 Module: OSPF Level: 2

An area border router did not send summary LSA messages via a PPP link when the area changed. This issue has been resolved.

PCR: 03568 Module: IPV6 Level: 3

IPv6 filters were not handling ICMPv6 packets correctly. This issue has been resolved.

PCR: 03571 Module: IPG Level: 3

The Proxy Arp default setting should be OFF for VLAN interfaces. This issue has been resolved.

The *dot1dStpPortForwardTransitions* value in the *dot1dBridge* MIB was not correctly incremented when STP transitioned a port to the forwarding state. This issue has been resolved.

PCR: 03573 Module: IPG Level: 2

It is now possible to configure an IP filter with the default route of 0.0.0.0. This allows BGP to control the default route for route distribution.

PCR: 03574 Module: STP Level: 4

The *dot1dStpInfoTopChanges* value in the *dot1dBridge* MIB was not correctly incremented when a topology change was detected by the bridge. This issue has been resolved.

PCR: 03576 Module: IPG Level: 2

When the device received a route from two separate sources to the same destination network, RIP only used the metric value when selecting the best route. RIP now selects the route by lowest preference value, or if they are the same, by the metric.

PCR: 03578 Module: SWI Level: 2

The DELETE SWITCH TRUNK PORT=ALL command was not returning the deleted trunk group ports to their pre-set port speed and duplex settings. This issue has been resolved.

PCR: 03582 Module: FIREWALL, IPG Level: 4

Previously, when the ADD FIREWALL POLICY INTERFACE command activated software routing, the static IP ARP entries were removed automatically. Static IP ARP entries now remain, and the following message is displayed:

```
WARNING: Static ARPs associated with a particular VLAN are
recommended to be deleted when Firewall is enabled on the VLAN.
```

PCR: 03583 Module: SWI Level: 3

New command added to enable a single selected blade to be reset.

```
RESET SWITCH BLADE={blade-number}
```

Where *blade-number* is a numeric from 1-8.

PCR: 03584 Module: MLD Level: 3

MLD had no mechanism for dealing with an IPv6 interface changing its local link address. This issue has been resolved.

PCR: 03587 Module: SWI Level: 2

Hot swapping blades occasionally caused fatal errors. Also, blade reinsertion was occasionally undetected. This issue has been resolved.

PCR: 03590 Module: DHCP Level: 2

The reclaim process was disrupted if, during this process, entries about to be reclaimed to static, were changed. DHCP static entries are now fully compatible with the normal reclaiming process.

PCR: 03592 **Module: FW** **Level: 3**

The GBLPORT parameter used when setting up a firewall NAT rule, has changed from a *mandatory*, to an *optional* parameter.

PCR: 03593 **Module: CORE, SNMP** **Level: 3**

Switchblade SNMP objects were previously accessible from within the Claymore SNMP MIB object. This issue has been resolved.

PCR: 03594 **Module: PING** **Level: 2**

IPv6Ping or Traceroute sometimes caused the device to restart. This issue has been resolved.

PCR: 03597 **Module: IPG** **Level: 2**

Replies to ARP requests were not always adding corresponding entries into the ARP table. This issue has been resolved.

PCR: 03599 **Module: CORE** **Level: 3**

If the settable temperature threshold was *undefined* and then set to a defined value using the SET SYSTEM TEMPTHRESHOLD command; an SNMP Trap, together with its corresponding log message, was generated. This occurred whenever the current temperature was lower than the value defined. This issue has been resolved.

PCR: 03609 **Module: OSPF** **Level: 1**

The IP route filter did not always work correctly for OSPF. This issue has been resolved.

PCR: 03610 **Module: IPv6** **Level: 2**

The operation of the ADD IPV6 ROUTE command METRIC parameter has changed and now applies differently for statically and non-statically defined routes. Previously, an interface failure would cause this parameter to take one of two values, 16 for an inactive interface, and 1 once it returned to the active state.

For statically defined routes, the parameter will now keep its configured value, regardless of the interface state.

For non-aesthetically defined routes, the parameter will now take the value 16 only when the interface is inactive. Once the interface returns to an active state, the parameter's configured value will be applied.

PCR: 03614 **Module: SWI** **Level: 2**

Setting internal IP and IPX addresses using the SET SWI BLADE [IP=ip-add] [IPX=ipx-add] command, had no effect on the IP and IPX tables. This issue has been resolved.

PCR: 03615 **Module: OSPF** **Level: 1**

Zmodem uploads to certain terminal emulators were failing because of an incorrect 16-bit checksum. This issue has been resolved.

PCR: 03618 **Module: DHCP** **Level: 3**

The SHOW DHCP CLIENT command output showed a *ClientId* value even when the *State* for the client entry was *Unused*. This issue has been resolved.

PCR: 03619 **Module: IPv6** **Level: 4**

When the SET IPv6 FILTER command specified a filter that did not exist, an `Operation successful` message was displayed as well as an error message. This issue has been resolved.

PCR: 03620 **Module: IPV6** **Level: 3**

The 16-bit reserved field after the maximum response code field was not set to zero, as specified by the Internet Draft "*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*". This issue has been resolved.

PCR: 03621 **Module: IPG** **Level: 3**

At startup, the switch was not sending or receiving a complete set of linktrap messages. This issue has been resolved.

PCR: 03624 **Module: IPV6** **Level: 3**

The ADD IPV6 FILTER and SET IPV6 FILTER commands accepted a SESSION parameter when the PROTOCOL parameter was not TCP. The SESSION parameter specifies the type of TCP packet to match. This issue has been resolved.

PCR: 03625 **Module: STP, SWI** **Level: 4**

The MIB object *dot1dStpTimeSinceTopologyChange* has been implemented to record when a topology change is detected by the bridge.

PCR: 03626 **Module: CLASSIFIER** **Level: 3**

The ETHFORMAT parameter, of the CREATE CLASSIFIER command, was accepting unsupported values. This issue has been resolved.

PCR: 03628 **Module: IPV6** **Level: 3**

The IPv6 priority filter was not working in SwitchBlade and AT-9800 Series Switches. This issue has been resolved.

PCR: 03633 **Module: SWCX** **Level: 3**

The IPv6 neighbour cache was not clearing when the interface was either disconnected or failed. Now, when an interface either fails or is disconnected, the neighbour cache is cleared after a short delay.

PCR: 03637 **Module: IPV6** **Level: 1**

IPv6 static tunnels remained in the Tentative state and did not change to the Preferred state. This issue has been resolved.

PCR: 03642 **Module: SWI** **Level: 3**

The SHOW SWITCH command INSTANCE parameter was not being accepted. This issue has been resolved.

PCR: 03644 **Module: SNMP** **Level: 3**

The MAC port counters were not updating as the port received and transmitted its packets. This resulted in the SNMP switch interface counters remaining unchanged. This issue has been resolved.

PCR: 03646 **Module: IPv6** **Level: 1**

A fatal error occurred when the SHOW IPV6 MLD INTERFACE command was executed after the interface had been destroyed. This issue has been resolved.

PCR: 03647 **Module: SNMP** **Level: 2**

A fatal error occurred when a *Set* request with an incorrect object ID value was received by SNMPv2c. This issue has been resolved.

PCR: 03648 **Module: CORE** **Level: 3**

Fans on some AT-9800 Series switches were taking too long to speed up and was causing the fault LED to flash for the first 10 seconds. This issue has been resolved.

PCR: 03650 **Module: IPG** **Level: 3**

IGMP *Query* messages were sent over an interface even if IGMP had been disabled on that interface. This issue has been resolved.

PCR: 03653 **Module: SWI** **Level: 3**

SwitchBlade port numbers were displayed in the MIB using absolute port numbering. This display has been changed to a 1000 based, port numbering system, where the first digit identifies the card and the other three digits identify the port on the card.

PCR: 03654 **Module: SWI** **Level: 1**

Ports were enabled before the switch was completely initialised. This sometimes caused the switch to fail when restarted under high load. This issue has been resolved.

PCR: 03657 **Module: SWI** **Level: 3**

Executing the DISABLE SWITCH PORT command on a port that was the source of a mirror port did not disable the mirror port. This issue has been resolved.

PCR: 03658 **Module: SWI** **Level: 3**

The CREATE CONFIG command placed the DISABLE SWITCH HASH=L3,L4 command in the wrong section. This issue has been resolved.

PCR: 03659 **Module: FILE** **Level: 3**

Invalid characters could be used in the SHOW CF DIR command. This issue has been resolved.

PCR: 03660 **Module: SWI** **Level: 3**

On the SwitchBlade, it was not possible to perform a GET or GET NEXT in order to retrieve bridge information.

PCR: 03662 **Module: IPG** **Level: 1**

Equal Cost Multi-Path (ECMP) routing selected a route with an infinite metric, so that forwarded packets using that route were discarded. This issue has been resolved.

PCR: 03666 **Module: BGP** **Level: 3**

BGP advertised interface routes when the corresponding interface was down. This issue has been resolved.

PCR: 03667 **Module: IP, ARP** **Level: 3**

Module: IP ARP Network Affecting: No

Port numbers were being listed incorrectly in the log file. This issue has been resolved.

PCR: 03669 **Module: FIREWALL** **Level: 3**

If the firewall received a packet with an incorrect TCP checksum and ACK number, the packet was sent to the client. Such packets are now rejected by the firewall. This patch fixes the problem.

PCR: 03679 **Module: IPG** **Level: 3**

When IP filters were deleted, the corresponding IP flow cache was not invalidated. This issue has been resolved.

PCR: 03669 **Module: FIREWALL** **Level: 3**

If the firewall received a packet with an incorrect TCP checksum and ACK number, the packet was sent to the client. Such packets are now rejected by the firewall.

PCR: 03670 **Module: SWCX** **Level: 4**

Resetting the switch port counters also reset the interface level counters. Sometimes this caused the interface counters to be incorrect. This issue has been resolved. Note: The interface SNMP MIB counters are not reset when the interface counters are reset via the command line.

PCR: 03675 **Module: SWI** **Level: 2**

It was possible for buffer leaks to occur when exchanging line cards that were receiving CPU traffic. This issue has been resolved.

PCR: 03677 **Module: SYSR** **Level: 2**

SYSR error messages were causing the console to lock up. This issue has been resolved.

PCR: 03683 Module: SWCX Level: 2

Jumbo packets could not be enabled on some ports of the 48 port line cards. This issue has been resolved.

PCR: 03685 Module: SWI Level: 2

CAM reads and writes were sometimes corrupted if generated whilst address learning was in progress. The result could be table corruption and unrecoverable lock up. This issue has been resolved.

PCR: 03690 Module: CORE Level: 3

The SET SYS RPS=ON command is no longer supported on the SwitchBlade. A message advising this, will now appear in the terminal

PCR: 03692 Module: BGP Level: 2

Occasionally a fatal exception may have occurred when sending BGP aggregate routes. This issue has been resolved.

PCR: 03694 Module: SWCX Level: 2

Port queues were not being cleared when their ports went down. This was resulting in a variety of problems. This issue has been resolved.

PCR: 03696 Module: IPG Level: 2

IGMP snooping entries were not being deleted from the hardware table. This issue has been resolved. Also, port timers are now updated when the IGMP timeout is changed.

PCR: 03697 Module: SWI Level: 2

Fatal errors occurred on occasions when mirroring was enabled. This issue has been resolved.

PCR: 03698 Module: DVMRP Level: 3

The output of the SHOW DVMRP FORWARDING command did not display the forwarding ports. This issue has been resolved.

PCR: 03700 Module: STP Level: 2

Fatal errors occurred when hotswapping a line cards that were running Rapid STP mode. This issue has been resolved.

PCR: 03704 Module: BGP Level: 2

BGP was importing the best route from IP without checking whether the route was *reachable*. BGP now selects the best *reachable* route. If there are no *reachable* routes, BGP will select the best *unreachable* route.

PCR: 03707 Module: STP Level: 2

When adding a port to a VLAN, any STP ports that had been disabled in the default STP were re-enabled. This issue has been resolved.

PCR: 03708 Module: DHCP Level: 2

When the DELETE DHCP RANGE command was executed, DHCP attempted to reclaim the addresses in that range. It also tried to reclaim

addresses in that range that were not allocated at that time, resulting in duplicate addresses appearing on the free list for allocation. This has been resolved by allowing DHCP to reclaim only those addresses that are currently in use by one of its clients.

PCR: 03709 Module: SWCX Level: 3

The PM table portmap was being updated each time a port was unplugged or a link went down.

PCR: 03712 Module: SW Level: 3

The port security feature of limiting the number of MAC addresses learned on a port, was including static address entries even with the ADD SWITCH FILTER command LEARN parameter set to *default*. This issue has been resolved.

PCR: 03716 Module: STP Level: 3

When AT-9800 Series switches, were operated in rapid STP mode, the point to point field was not updating when speed or duplex changes occurred to a port. This issue has been resolved.

PCR: 03720 Module: STP Level: 1

When changing from RSTP to STP mode, the STP command RSTPTYPE parameter was still appearing in the SHOW DYNAMIC command output. This issue has been resolved so that the RSTPTYPE parameter is no longer displayed in the command output.

Also when changing between RSTP and STP modes, disabled STP ports were not remaining in the disabled state. This issue has also been resolved.

PCR: 03720 Module: STP Level: 2

When changing from RSTP to STP mode, the STPCOMPATIBLE option for the RSTPTYPE parameter incorrectly appeared in the dynamic configuration. Also, when changing from RSTP to STP mode or vice versa, disabled STP ports did not remain in the disabled state. These issues have been resolved.

PCR: 03723 Module: BGP Level: 2

BGP routes that were added after a summary aggregate route had been formed were not suppressed. This issue has been resolved: all routes added after summary aggregate route creation are also now suppressed.

The SHOW BGP ROUTE command displayed unselected routes as the "best" route, until they had been processed. This issue has been resolved.

When a single route was deleted from an aggregate route, the aggregate route was deleted, even if it contained other routes. This issue has been resolved.

PCR: 03725 Module: SWCX Level: 3

The maximum Layer 3 throughput across line cards was only 25% under some circumstances. This issue has been resolved.

PCR: 03728 Module: IPG Level: 4

A field has been added to the SHOW IP command output that displays whether the IP ARP log is enabled or disabled.

Features in SB251-08

Patch file details are listed in Table 2:

Table 2: Patch file details for Patch SB251-08.

Base Software Release File	so-251.rez
Patch Release Date	14-May-2003
Compressed Patch File Name	sb251-08.paz
Compressed Patch File Size	86524 bytes

Patch SB251-08 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 03251 Module: SWI Level: 2

A fatal error occurred when the ADD SWITCH TRUNK command specified an invalid port. This issue has been resolved.

PCR: 03414 Module: SWI Level: 2

A fatal error occurred when removing a line card from a SwitchBlade if STP was enabled. This issue has been resolved.

PCR: 03466 Module: SWI Level: 2

System performance was low when adding large numbers of entries to CAM. This issue has been resolved. CAM is now initialised to allow better performance, especially for the addition of ARP and IP entries.

PCR: 03470 Module: SWI Level: 2

The DELETE SWITCH TRUNK PORT command could cause an unrelated port to stop forwarding packets, or learn new MAC addresses. This issue has been resolved so that unrelated ports are not affected by the trunk group port deletion.

PCR: 03509 Module: SWI Level: 2

All IP routes were being added to all switch instances. This caused issues on SwitchBlade line cards that did not have enough CAM to store the routes, and the line card did not always need every route. IP routes are now only added:

- to a switch instance if the route was learned on that instance
- if the route is for an interface
- if the route was added statically, or
- if the switch instance has a CAM which is the same size or larger than the CAM of the switch instance that the route was learned on.

PCR: 03518 Module: SWI Level: 3

An issue exists where the CAM entry 0 in the VLAN Tag table is either not updated or is being over written with invalid data. This PCR adds debugging to trace the fault.

Features in SB251-07

Patch file details are listed in Table 3:

Table 3: Patch file details for Patch SB251-07.

Base Software Release File	sb-251.rez
Patch Release Date	22-Apr-2003
Compressed Patch File Name	sb251-07.paz
Compressed Patch File Size	86524 bytes

Patch SB251-07 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 03399 Module: STP, SWI Level: 1

With this enhancement:

- STP and Port Trunking now work together correctly.
- BDPUs Forwarding is implemented. The BDPUs Forwarding feature configures the switch to forward all received STP BDPUs. Under normal circumstances, the switch will not forward any received STP BDPUs, even if STP is enabled.

This implementation is for standard STP, it does not guarantee that RSTP and port trunking will work correctly together in all situations.

STP does not update the pathcost for trunked ports, which means that a trunk group has the same pathcost as a single port. This may cause STP Blocking where it is not expected. To overcome this, the user should explicitly set the pathcost for the trunk group ports to be less than the default value for a single port.

STP reconfigures if the Master port in a trunk group goes link down. If the Master port in a trunk group goes link down, and a Non-Master port is still link-up, then STP will go through the Listening>Learning>Forwarding reconfiguration on the new Master port. This means that there will be a switching outage on the trunk group whilst the new Master port transitions to the Forwarding state.

Command handler changes:

- The PORT parameter of the CREATE SWITCH TRUNK PORT and ADD SWITCH TRUNK PORT commands must specify ports that have identical STP port configurations.
- The ENABLE STP and ENABLE STP PORT commands cannot be used to enable STP operation on a port that has been disabled from STP operation because of Port Trunking. Only the Master port in a trunk group actively participates in the STP algorithm. Non-Master ports in the trunk group are in the STP Disabled State.
- The output for the SHOW STP PORT command has been modified so that Non-Master Ports in a trunk group do not take part in the STP algorithm.

- The output for the SHOW STP PORT command has been modified so that it displays whether a user has set the PATHCOST value, or if it was auto-configured.
- The PORT parameter of the SET STP PORT command specifies either all the ports in a trunk group, or none of the ports in a trunk group.
- The STPFORWARD parameter has been added to the ENABLE SWITCH and DISABLE SWITCH commands. If STPFORWARD is enabled, and there is no enabled STP instance, then the switch will forward all received BPDUs. If STPFORWARD is enabled, and an STP instance is enabled, then STPFORWARD will be disabled by default and a message will be generated.
- The SHOW SWITCH command now shows the status of the BPDU Forwarding feature.

PCR: 03401 Module: SWI

An enhancement has been made to the Test module to optimise the reception of the loopbacked packets that are used to confirm operation of the switch ports.

Features in SB251-06

Patch file details are listed in Table 4.

Table 4: Patch file details for Patch SB251-06.

Base Software Release File	sb-251.rez
Patch Release Date	10-Apr-2003
Compressed Patch File Name	sb251-07.paz
Compressed Patch File Size	79684 bytes

Patch SB251-06 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 03340 Module: SWI, SYSR Level: 1

After a power cycle, or a reboot command, the SwitchBlade would occasionally repeatedly restart if it had two active controller cards. Also, the Slave controller card would sometimes not take over if the Master controller card failed.

Features in SB251-05

Patch file details are listed in Table 5.

Table 5: Patch file details for Patch SB251-05.

Base Software Release File	sb-251.rez
Patch Release Date	31-Mar-2003

Table 5: Patch file details for Patch SB251-05.

Compressed Patch File Name	sb251-05.paz
Compressed Patch File Size	71096 bytes

Patch SB251-05 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 03281 Module: SWI Level: 2

Specifying the PORT and SPEED parameters with the CREATE SWITCH TRUNK command did not set ports in a trunk group to advertise the correct trunk group speed and duplex mode. This issue has been resolved.

PCR: 03313 Module: SWI Level: 1

A power cycle on the switch could cause the console port to become frozen if a port was in a link up state. If a port went into a link down state, then the console port became unfrozen. If RESTART REBOOT or RESTART SWITCH commands were used, then the console port functioned correctly. This issue has been resolved.

Features in SB251-04

Patch file details are listed in Table 6.

Table 6: Patch file details for Patch SB251-04.

Base Software Release File	sb-251.rez
Patch Release Date	24 -Mar-2003
Compressed Patch File Name	sb251-04.paz
Compressed Patch File Size	71112 bytes

Patch SB251-04 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 03226 Module: SWI Level: 2

An internal misconfiguration of memory occurred when an M3 control card and an M5 control card were installed, and the M3 control card was acting as the Master. This could cause unexpected restarts. This issue has been resolved.

PCR: 03228 Module: SWI Level: 1

On a 48 port line card, or a 32F card, if Port 1 went down, or was disconnected, then traffic on Port 13 was also stopped, and vice versa. The same issue affected other pairs of ports. This issue has been resolved.

PCR: 03230 Module: SWI Level: 2

Port speeds on trunk ports sometimes had to be set using the SET SWITCH PORT command instead of automatically adopting the trunk group speed. If a port was added to a trunk group and the port status was 'up', (that is, it

was correctly connected to another port) then the trunk group speed should have applied to all the ports in the trunk, but it did not. Similarly, if a port was added to a trunk group, and the port status was 'down', but it was later linked correctly, then the trunk group speed should have applied to the ports in the trunk. This issue has been resolved.

PCR: 03243 Module: SWI Level: 2

After auto negotiation had finished between two ports, the port on the SwitchBlade would not show link up status when the SHOW SWITCH PORT command was executed. The auto negotiation process is now restarted if auto negotiation is completed and the link is shown as down.

PCR: 03249 Module: SWI Level: 4

The LEDs on line cards now continue to flash when activity exists. Previously if a cable was connected and disconnected to Line 48 and G8 ports, with traffic being transmitted from the other end, then the LED would stop flashing, even when there was activity on the link.

Features in SB251-03

Patch file details are listed in Table 7.

Table 7: Patch file details for Patch SB251-03.

Base Software Release File	sb-251.rez
Patch Release Date	12-Mar-2003
Compressed Patch File Name	sb251-03.paz
Compressed Patch File Size	68784 bytes

Patch SB251-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 02361 Module: SWI Level: 4

The SwitchBlade mirror port field on the second instance of a switch chip was displaying as though it was the first instance. For example, if 2.26 was configured as the mirror port, the GUI mirror object would return 2.2. The first chip instance was not affected. This issue has been resolved.

PCR: 02527 Module: TCP Level:3

TCP6 did not send a *TCP Reset* message under some circumstances, for example when the Telnet server was disabled. This issue has been resolved.

PCR: 03025 Module: GUI Level:2

A buffer address was incrementing and not returning buffers for reuse when the command line interface was accessed via the GUI interface. This issue has been resolved.

PCR: 03055 Module: SWI Level: 4

If the SET SWITCH BLADE command was executed with the default settings, then the default settings were added to the configuration file. The

SET SWITCH BLADE settings are now only added to the configuration file if they differ from the default settings.

PCR: 03060 **Module: CORE, SWI** **Level: 3**

Support has been added, to the MIB-2 interface MIB, for the port interface. This means that port counters can now be shown.

PCR: 03066 **Module: SWI** **Level: 2**

If a hardware filter was added to the switch, with a source VLAN and a destination port of 1, then a host connected to the switch could not PING a host on a different port. This issue has been resolved.

PCR: 03071 **Module: CORE** **Level: 2**

An unexpected restart that occurred when upgrading a SwitchBlade from Release 2.4.4 to Release 2.5.1 was caused by NVS generating an SNMP trap. This issue has been resolved.

PCR: 03079 **Module: IPG, SWI** **Level: 1**

Static routes were occasionally not added to all hardware tables across all instances. This would affect connectivity if an instance had a default route added to its table that pointed out one of its ports. This issue has been resolved.

PCR: 03088 **Module: SWI** **Level: 2**

Ports could not be added to the default VLAN after a hotswap, if the default VLAN was Protocol, Subnet, MAC address, or Limited protocol based. This issue has been resolved.

PCR: 03105 **Module: FIREWALL** **Level: 3**

Incorrect handling of TCP sessions, and poor load balancing performance could be caused by TCP virtual balancers not selecting a new resource if required. This issue has been resolved.

PCR: 03112 **Module: IPV6** **Level: 3**

The ADD IPV6 ND command now has a PORT parameter which means that it can be associated with the VLAN parameter.

PCR: 03118 **Module: CORE** **Level: 4**

Changes have been made to the *SysDescription*.

PCR: 03119 **Module: CLASSIFIER** **Level: 4**

TCP source and TCP destination ports were swapped when viewed in the GUI. This issue has been resolved.

PCR: 03138 **Module: SWI** **Level: 2**

Packets that were sent out a default route could have an incorrect source IP address, if the interface route to the destination IP address existed but was down. This issue has been resolved.

PCR: 03141 **Module: IPG** **Level: 3**

Packets could be sent with an incorrect source address if a route was added to a VLAN and another VLAN had an IP interface configured that was in the same subnet as the route. This issue has been resolved.

PCR: 03142 Module: SWI Level: 1

If a BIST was run at low temperatures, for example 5 or 10 degrees Celsius, on a G8 card, then a watchdog timer restart could occur. The switch now checks for the real course of the external interrupts that occur when running BIST.

PCR: 03148 Module: IPG Level: 3

If the Gratuitous ARP feature was enabled on an IP interface, and an ARP packet arrived, (either ARP request, or reply) that had a Target IP address that was equal to the sender's IP address, then the ARP cache was not updated with the ARP packet's source data. This issue has been resolved.

PCR: 03191 Module: SWI Level: 1

If two line cards were inserted in quick succession, then a software restart could occasionally occur. This issue has been resolved.

PCR: 03192 Module: SWI Level: 2

When the Built-In Self Test was run, a fault would occasionally be reported which said that a MAC address was not learnt during the loopback test. The ports in the BIST loopback test now remain in loopback.

Features in SB251-02

Table 8: Patch file details for Patch SB251-02.

Base Software Release File	sb-251.rez
Patch Release Date	25-Jan-2003
Compressed Patch File Name	sb251-02.paz
Compressed Patch File Size	48608 bytes

Patch SB251-02 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 02553 Module: SWITCH Network affecting: No

64 bit MIB counters were not incremented or cleared for port interfaces. This issue has been resolved.

PCR: 02574 Module: DVMRP Network affecting: No

Some change actions, and the resending of prune messages were not operating correctly. This issue has been resolved.

PCR: 02582 Module: SWI Network affecting: No

Pause flow control is now disabled by default on all ports. This improves performance of the switch when it is congested.

The DPORT parameter in the ADD SWITCH HWFILTER command was omitted when the configuration was generated. This issue has been resolved.

PCR: 03023 Module: SWI Network affecting: No

The SET SWITCH PORT ACCEPTABLE command did not work correctly on all specified port numbers. This issue has been resolved.

PCR: 03028 Module: SWI Network affecting: No

A warning message was generated when a slave line card was not initialised, and the configuration script was not loaded. This issue has been resolved.

PCR: 03030 Module: SWI Network affecting: No

RIP was not operating correctly because a MAC address search returned the wrong port number. This issue has been resolved.

PCR: 03031 Module: FIREWALL Network affecting: No

The ADD FIREWALL POLICY RULE command included an erroneous check on port ranges for non-NAT rules. This check is now restricted to NAT rules.

PCR: 03034 Module: SWI Network affecting: No

Executing the SET IP INTERFACE and SET IPX INTERFACE commands on a SwitchBlade produced debugging output on the ASYN port. This issue has been resolved.

PCR: 03037 Module: QOS Network affecting: No

A new value is now shown in the output of the SHOW QOS POLICY command. This is the value of the port bandwidth used when the default traffic class percentage bandwidth is set on a QoS Policy.

PCR: 03039 Module: SWITCH, IPG Network affecting: No

Adding a layer 2 filter on a SwitchBlade did not block traffic to the end host as intended. This issue has been resolved.

PCR: 03043 Module: SWITCH Network affecting: No

On a SwitchBlade, PCI errors occurred periodically after a line card was hotswapped. This issue has been resolved.

PCR: 03047 Module: CORE Network affecting: No

The board revision number for the slave control blade was erroneously set to the same number as the master control blade. This issue has been resolved.

PCR: 03428 Module: STP Network affecting: No

If a port belongs to an enabled STP instance, but the port has been disabled from STP operation with the DISABLE STP PORT command, the port will not respond to ARP requests. This patch implements a workaround that allows disabled STP ports to respond to ARP requests.

Features in SB251-01

Patch file details are listed in Table 9:

Table 9: Patch file details for Patch SB251-01.

Base Software Release File	sb-251.rez
Patch Release Date	15-Jan-2003
Compressed Patch File Name	sb251-01.paz
Compressed Patch File Size	71828 bytes

PCR: 02555 Module: SWI Network affecting: No

Layer 2 filtering is now working correctly.

PCR: 02561 Module: SWI Network affecting: No

32 bit counters now only show 8 bit contents.

PCR: 02563 Module: SWI Network affecting: No

The IPM (Layer 3 Multicasting table) now updates correctly to add or delete the ingress linecard to control blade ports, and the control blade to egress linecard ports when updating forwarding.

PCR: 02568 Module: CORE Network affecting: No

The ENABLE SYSTEM SECURITY_MODE command was enabling the system security mode, but after the switch was restarted the system security mode was disabled again. Also, when NVS was re-initialised because, for example a battery had been exhausted, the system could not make an SNMP trap. These issues have been resolved.

PCR: 02576 Module: SWI Network affecting: No

When the DISABLE SWITCH PORT FLOW=PAUSE command was executed on a port or ports, they would still appear to be enabled at a higher level. This issue has been resolved.

PCR: 02396 Module: DHCP Network affecting: No

DHCP RENEW request messages are now unicast (as defined in the RFC), not broadcast.

PCR: 02575 Module: SWI Network affecting: No

VLAN tagged multicast packets were incorrectly being sent over untagged VLAN interfaces. This issue has been resolved.

PCR: 02574 Module: DVMRP Network affecting: No

Some change actions, and the resending of prune messages were not operating correctly. This issue has been resolved.

PCR: 02582 Module: SWI Network affecting: No

Pause flow control is now disabled by default on all ports. This improves performance of the switch when it is congested.

PCR: 02587 Module: OSPF Network affecting: No

When OSPF was enabled on startup, an OSPF interface would sometimes stay in the DOWN state. This issue has been resolved.

PCR: 03001 Module: SWI CLASSIFIER Network affecting: No

The following parameters have been changed CREATE CLASSIFIER, SET CLASSIFIER and SHOW CLASSIFIER commands:

- The MACTYPE parameter has been changed to MACTYPE={L2UCAST | L2MCAST | L2BCAST | ANY}. This resolves an error with internal hardware tables.
- The number of user-specified protocols in the PROTOCOL parameter has been increased from three to seven.
- The minimum value of the IPXDADDRESS parameter has been decreased from 10000000 to 00000001.

PCR: 03006 Module: SWI Network affecting: No

An issue which sometimes resulted in a broadcast storm within the internal ports on the SwitchBlade, a reduction in bandwidth, and a loss of pinging has been resolved.

PCR: 3008 Module: SWI Network affecting: No

An issue which caused pings to fail when a control card was inserted in the left hand slot to act as a slave, has been resolved.

PCR: 03014 Module: IPG, SWI Network affecting: No

Support has been added to allow for multicasting to any number of overlapping VLANs up to the maximum number of multicast forwarding entries.

PCR: 03018 Module: SWI Network affecting: No

An issue with pings failing after network host routes disappeared from the switch due to an IP hashing error has been resolved.

PCR: 03020 Module: SWI Network affecting: No

An issue with an interrupt occurring when waiting on the MDIO which caused the MDIO to read or write incorrect information has been resolved.

PCR: 03021 Module: SWI Network affecting: No

Ping would sometimes not work correctly after a 48 line card was extracted, and after a restart reboot. This issue has been resolved.

Availability

Patches can be downloaded from the Software Updates area of the Allied Telesyn web site at www.alliedtelesyn.co.nz/support/updates/patches.html. A licence or password is not required to use a patch.